Configuring Remote Access

Router Software Version 11.00 Rev. 4n
Site Manager Sofware Version 5.00 Rev. 4n

Part No. 114084 Rev. A
November 1996

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA.November 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA Requirements Only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment generates, uses, and can radiate radio-frequency energy. If you do not install and use this equipment according to the instruction manual, this product may interfere with radio communications. This product has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Operating this equipment in a residential area is likely to interfere with radio communications; in which case, the user, at his/her own expense, must correct the interference.

Shielded-compliant cables must be used with this unit to ensure compliance with the Class A limits.

European Requirements Only

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class A (CISPR 22:1985/BS 6527:1988).

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class B (CISPR 22:1985/BS 6527:1988).

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で、商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域、その隣接地域等で使用した場合、ラジオ、テレビ受信機等に障害を与えることがあります。

上記基準に適合する遮蔽ケーブルをご自分でお求めになり、取扱説明書に従って、正しくご使用ください。

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the 1st category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Compliance with the applicable regulations is dependent upon the use of shielded cables. The user is responsible for procuring the appropriate cables. Read instructions for correct handling.

Canada Requirements Only

Canada CS-03 Rules and Regulations

Note: The Canadian Department of Communications label identifies certified equipment. The certification means that the equipment meets certain telecommunications network protective operations and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent the degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Canada CS-03 — Règles et règlements

Note: L’étiquette du ministère des Communications du Canada indique que l’appareillage est certifié, c’est-à-dire qu’il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l’appareillage fonctionnera à la satisfaction de l’utilisateur.

Avant d’installer l’appareillage, s’assurer qu’il peut être branché aux installations du service de télécommunications local. L’appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d’un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu’une telle installation n’assure pas un service parfait en tout temps.

Les réparations de l’appareillage certifié devraient être confiées à un service d’entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l’utilisateur ou de mauvais fonctionnement de l’appareillage, le service de télécommunications peut demander le débranchment de l’appareillage.

Pour leur propre sécurité, les utilisateurs devraient s’assurer que les mises à la terre des lignes de distribution d’électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

D. O. C. Explanatory Notes: Equipment Attachment Limitations

The Canadian Department of Communications label identifies certified equipment. This certification meets certain telecommunication network protective, operational and safety requirements. The department does not guarantee the equipment will operate to the users satisfaction.

Before installing the equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Notes explicatives du ministère des Communications: limites visant les accessoires

L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d'un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchment de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Réglement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Réglement sur le brouillage radioélectrique du ministère des Communications du Canada.

T1 Service Compliance Statements

T1 Service

NOTE: This T1 Service notice applies to you only if you have received a single or dual port Multi-Channel T1 (MCT1) Link Module (which provides an internal CSU).

This equipment complies with Part 68 of FCC Rules. Please note the following:

1. You are required to request T1 service from the telephone company before you connect the CSU to a T1 network. When you request T1 service, you must provide the telephone company with the following data:
   - The Facility Interface Code

     Provide the telephone company with both codes below:

     — 04DU9-B (1.544 MB D4 framing format)
     — 04DU9-C (1.544 MB ESF format)

     The telephone company will select the code it has available.
   - The Service Order Code: 6.0F
   - The required USOC jack: RJ48C
   - The make, model number, and FCC Registration number of the CSU.
2. Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. The telephone company will notify you in advance of such changes to give you an opportunity to maintain uninterrupted telephone service.
3. If your CSU causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible and will be informed of your right to file a complaint with the FCC.
4. If you experience trouble with the CSU, please contact Bay Networks Technical Response Center in your area for service or repairs. Repairs should be performed only by service personnel authorized by Bay Networks, Inc.

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-96-69-68
Sydney, Australia	(61) 2-9927-8880
Tokyo, Japan	(81) 3-5402-7041
5. You are required to notify the telephone company when you disconnect the CSU from the network and when you disconnect the BCNX or BLNX from the network.

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Before You Begin xxi
Where to Find AN, ANH, or ARN Information xxii
Conventions xxiii
Acronyms xxiv
Ordering Bay Networks Publications xxv

Technical Support and Online Services

Bay Networks Customer Service xxviii
Bay Networks Information Services xxix
World Wide Web xxix
Customer Service FTP xxix
Support Source CD xxx
CompuServe xxx
InfoFACTS xxxi
How to Get Help xxxi

Chapter 1
Understanding Tools and Options

Software Management Tools 1-1
Router Software 1-2
Boot Configuration Options 1-3
The Boot Process 1-6
Network Boot 1-6
Getting an IP Address 1-6
Getting Kernel Image and Configuration Files 1-10
Local Boot 1-12
Configuring the Initial IP Interface 1-13

Chapter 2
Selecting the Boot Configuration

Booting the Router for the First Time 2-1
EZ-Install 2-2
Netboot 2-2
Local Boot 2-3
Recommendations 2-3
Booting the Router Routinely 2-3
Netboot 2-3
Directed Netboot 2-4
Local Boot 2-5
Recommendations 2-5
Completing a Startup Option 2-6
EZ-Install 2-6
Netboot 2-7
Directed Netboot 2-8
Local Boot 2-9

Chapter 3
Setting Up a UNIX Boot Server

Setting Up a BOOTP Server 3-2
Copying the BOOTPD Program on Sun Workstations 3-2
Setting Up BOOTP Sockets 3-2
Setting Up BOOTPD to Run 3-3
Setting Up BOOTPD to Respond to Routers 3-3
Editing the bootptab File 3-4
Verifying Consistent BOOTP Service 3-9
Setting Up a TFTP Server 3-9
Providing TFTPD Access to the Root Directory 3-9
Restricting TFTPD Access to a Specified Directory 3-10
Adding a TFTP User for an HP 9000 3-11
Setting Up Static Routes to Next-Hop Routers 3-11
Editing the inetd.conf File 3-12
Verifying the Routes 3-12
Loading the Changes into Memory 3-12
What to Do Next 3-13

Chapter 4
Configuring Network Booting

Preparing Configuration and Image Files 4-2
Creating Configuration Files 4-2
Preparing an Image 4-6
Enabling Netboot or Directed Netboot from Site Manager 4-7
Netboot and Directed Netboot Parameters 4-8
Configuring a Netboot or Directed Netboot Interface 4-11
Netboot Interface Parameters 4-14
Setting Up Routing Paths for Netboot 4-16
Enabling Router Interfaces 4-16
Creating BOOTP Relay Agent Forwarding Tables 4-17
BOOTP Relay Agent Interface Parameters 4-20
Creating the BOOTP Client Interface Table 4-21
BOOTP Client Interface Parameters 4-23

Chapter 5
Configuring the Router as a Network Boot Client

Working with a Person at the AN/ANH/ARN Site 5-2
Configuring the Router Boot Source 5-2
bconfig Command Format 5-2
bconfig Command Examples 5-3
Configuring the Netboot Interface 5-4
Configuring an IP Synchronous Interface for Network Booting 5-4
Configuring an Ethernet Interface for Network Booting 5-6
Configuring a Token Ring Interface for Network Booting 5-6
Enabling and Disabling Interfaces with ifconfig 5-7
ifconfig Command Examples 5-8
Verifying Your Configuration 5-9
What to Do Next 5-10

Chapter 6
Managing ANH Repeater Ports

Enabling and Disabling ANH Repeater Ports 6-1
Testing and Resetting ANH Repeater Ports 6-4
Repeater Port Group Parameter Descriptions 6-5

Chapter 7
Configuring a Data Collection Module

Ethernet DCM and RMON Overview 7-1
Remote Network Monitoring (RMON) 7-2
The RMON Groups 7-3
Ethernet Statistics Group 7-3
History Control Group and Ethernet History Group 7-4
Host Group 7-4
HostTopN Group 7-4
Matrix Group 7-4
Filter Group 7-4
Packet Capture Group 7-5
Alarm Group 7-5
Event Group 7-5
For More Information about RMON 7-5
Enabling a DCM Using Site Manager 7-6
DCM Global Parameter Descriptions 7-7
Managing the DCM Using Site Manager 7-11
Activating the DCM 7-12
Disabling the DCM 7-12
Booting the DCM 7-13
Changing the DCM Configuration Parameters 7-13
Deleting the DCM Software Subsystem 7-14
Managing the DCM Using the Technician Interface 7-15
Changing DCM Configuration Parameters 7-15
RMON Implementation Notes 7-16
RMON Applications 7-17
RMON Memory Use 7-18
Interoperability Issues and Memory Use for RMON Groups 7-18
Statistics Group 7-19
History Group 7-19
Host Group 7-20
HostTopN Group 7-21
Matrix Group 7-21
Filter and Capture Groups 7-22

Alarm and Event Group 7-23

Appendix A
Troubleshooting Network Boot Problems

Solving Startup Problems A-1
Router Fails to Get IP Address A-2
Upstream Router Not Receiving BOOTP Requests A-2
Upstream Router Not Sending BOOTP Responses A-2
Router Fails to Netboot A-3
Upstream Router Not Receiving BOOTP Requests A-3
Router Not Sending BOOTP Responses A-4
BOOTP Server Not Sending BOOTP Responses A-4
Router Fails to Perform Directed Netboot A-5
Router Netboots, but Fails to Load Applications A-5
Identifying Remote Connectivity Problems A-8
Displaying Messages from the AN/ANH/ARN Console A-8
Displaying Statistics and Error Messages A-8
Guidelines for Using Packet Capture A-9
Guidelines for Using a LAN Protocol Analyzer A-9
Resolving Connectivity Problems A-10
Displaying Parameter Settings A-10
Debugging the BOOTP Server A-12
Verifying the BOOTP Server Setup A-13
Displaying the BOOTP Server's IP Routes A-15
Displaying the Number of Packets Forwarded and Dropped A-15
Quick Get Instructions A-16
Technician Interface Instructions A-16
Maintaining the Router Software A-16
Upgrading the Software Image A-17
Restoring a Local File System A-17

Appendix B
Using the Local Boot Procedure

What Is Quick-Start? B-1
Using the Worksheets B-2
Global Information Worksheet B-3

Router Protocol Worksheets B-6
Wide Area Protocol Worksheets B-10
Running the Quick-Start Script B-14

Appendix C
Implementation Notes

Hints C-1
Notes C-2
Network Configuration Options C-3
Ensuring Ethernet Network Compliance C-3
Network Path Containing Three Repeaters C-4
Network Path Containing Four Repeaters C-4
Configuring a Single ANH C-4
Configuring Multiple Hubs C-6
Configuring an AUI Port C-7
Connecting the AUI Port to a Fiber Optic Backbone C-8
Connecting the AUI Port to a Coaxial Backbone C-9

Index

Figures

Figure 1-1. Getting an IP Address from a Bay Networks Standard Circuit or a Frame Relay PVC in Direct Access Mode 1-8
Figure 1-2. Getting an Address from a PVC in Group Access Mode 1-9
Figure 1-3. Getting the Pathnames of the Kernel and Configuration Files 1-10
Figure 1-4. Getting the Configuration File 1-11
Figure 1-5. Getting the Kernel 1-12
Figure 1-6. Establishing an IP Network Interface 1-13
Figure 3-1. Sample bootptab File 3-8
Figure 4-1. Edit Netboot Global Parameters Window 4-7
Figure 4-2. Netboot Interfaces Window 4-11
Figure 4-3. Netboot Interface Window 4-12
Figure 4-4. Netboot Interfaces Window 4-13
Figure 4-5. Enabling BOOTP in a Sample Network 4-16
Figure 4-6. BOOTP Relay Agent Interface Table Window 4-18
Figure 4-7. BOOTP Relay Agent Forwarding Table Window 4-19
Figure 4-8. BOOTP Addresses Window 4-19
Figure 4-9. BOOTP Client Interface Table Window 4-22
Figure 4-10. BOOTP Client Interface Address Window 4-22
Figure 6-1. 8-Port ANH Port Status Window 6-2
Figure 6-2. 12-Port ANH Port Status Window 6-3
Figure 6-3. Group Parameters Window 6-4
Figure 7-1. Edit Base Module DCM Parameters Window 7-6
Figure 7-2. Edit Base Module DCM Parameters Window 7-13
Figure B-1. Starting the IP Interface Test B-16
Figure C-1. Typical Single-ANH Configuration C-5
Figure C-2. Connecting the ANH with Other Hubs C-7
Figure C-3. Connecting Two ANH Systems Using 10Base-FL Transceivers C-8
Figure C-4. Connecting ANH Systems through a Coaxial Backbone C-9

Tables

Table 1-1. Summary of Boot Options 1-4
Table 3-1. BOOTPD Tags for a Router Hostname 3-5
Table 3-2. BOOTPD Tags for a Boot Image Name 3-6
Table 3-3. Providing TFTPD Access to Root and All Subdirectories 3-10
Table 3-4. Restricting TFTPD Access to One Directory 3-10
Table 4-1. BayStack AN Configurations 4-3
Table 4-2. BayStack ANH Configurations 4-4
Table 4-3. BayStack ARN Base Module Configurations 4-5
Table 4-4. BayStack ARN Expansion Module Configurations 4-5
Table 4-5. BayStack ARN Adapter Module Configurations 4-5
Table 5-1. bconfig Command Settings 5-3
Table 5-2. ifconfig Command Settings for a Synchronous Interface 5-5
Table 5-3. ifconfig Command Settings for an Ethernet Interface 5-6
Table 5-4. ifconfig Command Settings for a Token Ring Interface 5-7
Table 5-5. ifconfig Settings to Enable and Disable Netboot Interfaces 5-8
Table 7-1. DRAM and RMON Memory Size 7-18
Table 7-2. Maximum Number of Hosts 7-20
Table 7-3. Default Size for Capture Buffer 7-22
Table A-1. BOOTP Messages A-13
Table B-1. Quick-Start/Power-Start Commands B-15
Table C-1. IEEE 802.3 Maximum Segment Links C-4

About This Guide

Read this guide if you are responsible for connecting a Bay Networks™ BayStack™ Access Node (AN®), Access Node Hub (ANH™), or Advanced Remote Node (ARN™) router to a managed network.

This guide offers

- An overview of AN, ANH, and ARN software (Chapter 1)
- A description of network booting (Chapter 2)
- Instructions for setting up a UNIX workstation as a BOOTP server (Chapter 3)
- Instructions for configuring Site Manager to support network booting (Chapter 4)
- Instructions for configuring the router for network booting (Chapter 5)
- Instructions for managing ANH repeater ports (Chapter 6)
- Instructions for configuring an Ethernet Data Collection Module (DCM) for RMON statistics gathering (Chapter 7)
- Troubleshooting guidelines and procedures (Appendix A)
- Worksheets for completing the installation procedure (Appendix B)
- Implementation hints and notes (Appendix C)

Before You Begin

Before using this guide, you (or a person at the router site) must install the router, or hardware and network connections, as described in one of the following guides:

- *Installing and Operating BayStack AN and ANH Systems*
- *Installing and Operating BayStack ARN Routers*

Where to Find AN, ANH, or ARN Information

Use this guide in conjunction with other Bay Networks documentation to set up and manage AN, ANH, and ARN systems. Refer to the following when looking for specific information.

For Information on This	Look Here
Installing BayStack AN or ANH hardware	*Installing and Operating BayStack AN and ANH Systems*
Installing BayStack Advanced Remote Node hardware	*Installing and Operating BayStack ARN Routers*
Learning about AN, ANH, and ARN software and the four startup/boot options	Chapter 1 in this guide
Choosing a startup option for the router	Chapter 2 in this guide
Setting up a UNIX workstation as a BOOTP server to support a network boot option	Chapter 3 in this guide
Configuring Site Manager to support a network boot option	Chapter 4 in this guide
What to do at the AN/ANH/ARN site to support a network boot option	Chapter 5 in this guide
Configuring a Data Collection Module	Chapter 7 in this guide
Preparing for the Quick-Start (local boot) procedure	Appendix B in this guide
Completing any of the four startup options at the AN/ANH/ARN site	*Installing and Operating BayStack AN and ANH Systems* or *Installing and Operating BayStack ARN Routers*
Configuring and managing an AN/ANH/ARN after it is connected to the network	*Configuring Routers* and *Managing Routers and BNX Platforms*
Reconfiguring AN/ANH/ARN netboot interfaces	Chapter 5 in this guide
Considerations for setting up an AN/ANH/ARN	Appendix C in this guide
Resolving problems with the network boot process	Appendix A in this guide
Troubleshooting all other problems	*Troubleshooting Routers*

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &** Example: Use the **dinfo** command. Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AUI	Attachment Unit Interface
BOFL	Breath of Life
BOOTP	Bootstrap Protocol
BOOTPD	Boot Protocol Daemon
BRI	Basic Rate Interface
CHAP	Challenge Handshake Authentication Protocol
DCE	data communications equipment
DCM	Data Collection Module
DLCI	data link connection identifier
DLCMI	Data Link Control Management Interface
DTE	data terminal equipment
FTP	File Transfer Protocol
HDLC	high-level data link control
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPX	Internet Packet Exchange
ISDN	Integrated Services Digital Network
LMI	Local Management Interface
LQR	Link Quality Reporting
MAC	media access control
MAU	media access unit
MIB	management information base
MTU	maximum transmission unit
NBMA	nonbroadcast multi-access
NMM	network management module
OSPF	Open Shortest Path First Protocol
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PVC	permanent virtual circuit
RARP	Reverse Address Resolution Protocol

RFC	Request for Comments
RIP	Routing Information Protocol
RMON	remote monitoring
SAM	System Administration Manager
SMDS	switched multimegabit data service
SMIT	System Management Interface Tool
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TFTPD	Trivial File Transfer Protocol Daemon
UDP	User Datagram Protocol
UTP	unshielded twisted-pair

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Understanding Tools and Options

The Bay Networks BayStack ARN and AN families of routers connect multiprotocol workgroups to corporate backbone networks. This chapter provides an overview of the software tools and options for configuring remote access. The chapter includes information about the following:

- Software management tools
- Router software
- Boot configuration options
- Boot process

Software Management Tools

You configure and manage an AN, ANH, or ARN using

- The graphical, SNMP-based router management tools within *Optivity Internetwork*™, a component of the Bay Networks Optivity Enterprise™ application suite:
  - -- *Site Manager*, a router management, configuration, and monitoring application.
  - -- *RouterMan*™, a real-time router performance and status reporting appplication.
  - -- *PathMa*n™, a diagnostic application for determining the complete data path between any two network devices.
- The *Technician Interface*, a terminal-based command-line interface that operates in router memory. Technician Interface commands and scripts provide real-time SNMP-based MIB access from an attached or remote (modem or Telnet) console connection.

- A firmware diagnostics monitor with a command-line interface. You use the AN/ANH/ARN monitor to configure the router's boot configuration.

This manual describes how to configure the router's boot configuration using the Diagnostic Monitor and Technician Interface, and how to connect remote access systems to a managed network using Site Manager.

Router Software

Before it can operate, the AN, ANH, or ARN hardware must boot a *software image*. The software image is a group of executable files that operate the protocols that the network requires. The AN/ANH software image is called *an.exe*. The ARN software image is called *arn.exe*. The software image comprises the following executable startup files:

- A *krnl_an.exe* file (for the AN/ANH) or *krnl_arn.exe* (for the ARN) that contains the operating system kernel.
- Application files -- executable files needed to perform the functions specified in the configuration file. All application files have *.exe* filename extensions. (For example, the router needs an *ipx.exe* executable file to run IPX.)
- String files -- compressed ASCII files needed when you use the Technician Interface to display the event log or management information base (MIB) object names. Groups of string files remain in compressed format within the *an.exe* or *arn.exe* file until needed.

To bridge and route traffic, the AN, ANH, or ARN also needs a *configuration file* that is tailored to your network. A configuration file is a binary system file that contains hardware and software configuration data. The default configuration file is named *config*.

Boot Configuration Options

This section summarizes your options for getting the AN, ANH, or ARN software image and configuration files.

Note: If you plan to use the Quick2Config™ software to configure the AN or ANH, see *Configuring Your Router Using the Quick2Config Tool*. Quick2Config is a Microsoft Windows-based application that you can use to create or modify router configuration files.

An AN/ANH/ARN boots using one of four configured startup options. The differences among the four startup options are based on whether the router retrieves software image and configuration files over the network or from local memory.

Getting a software image or configuration file over the network is called *Netbooting*. Getting a file from the file system stored in local Flash memory is called *Local booting*.

To *initially* start up the AN, ANH, or ARN, you use one of these boot configuration options:

- EZ-Install (the default)
- Netboot
- Local Boot

To start up the AN, ANH, or ARN *after* the initial configuration, you use one of these options:

- Netboot
- Directed Netboot
- Local Boot

Table 1-1 summarizes the four startup options. The next section, "The Boot Process," describes how each option works.

Table 1-1. Summary of Boot Options

Boot Option	Source for Software Image	Source for config File	Description and Requirements
EZ-Install	Local (Flash memory)	Network (Serial connection)	The default option. The router boots from a software image in local memory, and then transmits a request for its IP address and configuration file through an attached serial interface. Next, a remote UNIX- or DOS-based workstation that is configured as a Boot Protocol (BOOTP) server downloads a customized configuration file; you save that configuration to Flash memory. Requires a communications link over an HDLC or Frame Relay interface. If EZ-Install fails, the router tries the Local Boot procedure.
Netboot	Network (Serial, Ethernet, or Token Ring* connection)	Network (Serial, Ethernet, or Token Ring* connection)	The router obtains all startup files from a remote UNIX- or DOS-based workstation that is configured as a BOOTP server. (Getting these files individually, rather than getting the entire *an.exe* or *arn.exe* file, minimizes the cost of line usage and prevents saturation of the router's memory.) Requires a local *an.exe* file (for the AN or ANH) or *arn.exe* file (for the ARN), a local console connection, and a communications link over an HDLC, Frame Relay, Ethernet, or (for the ARN)Token Ring* interface. If Netboot fails, the router tries the Local Boot procedure.

(continued)

Table 1-1. Summary of Boot Options *(continued)*

Boot Option	Source for Software Image	Source for config File	Description and Requirements
Directed Netboot	Network (Serial, Ethernet, or Token Ring* connection)	Network (Serial, Ethernet, or Token Ring* connection)	The router obtains all startup files from a remote UNIX- or DOS-based workstation that is configured as a Trivial File Transfer Protocol (TFTP) server. You specify the IP address of the TFTP server and the pathname of the startup files before booting. Requires a local *an.exe* file (for the AN or ANH) or *arn.exe* file (for the ARN), a local console connection, and a communications link over an HDLC, Frame Relay, Ethernet, or Token Ring* interface. If Directed Netboot cannot retrieve the appropriate files, the router attempts normal Netboot. If this fails, the router tries Local Boot.
Local Boot	Local (Flash memory)	Local (Flash memory)	The router boots using a software router image and configuration file stored in local memory. During the initial startup, the router uses a generic startup configuration file. You customize the default configuration file by assigning an IP address to an interface and running an installation script; this is called the *Quick-Start* procedure. Quick-Start requires a local console and an active IP network connection.

*. You can use the Netboot and Directed Netboot procedure on a Token Ring interface on the ARN only.

The Boot Process

An AN, ANH, or ARN boots using its configured startup option. The default configuration is *EZ-Install*.

(If an initial boot attempt fails on an AN or ANH, the router attempts to boot once using a different option. If both boot attempts fail, you must troubleshoot the problem and reboot the router as described in Appendix A. If an initial boot attempt fails on an ARN, the router first tries to local boot, and then netboot. The ARN continues attempts to local boot and netboot until it successfully boots.)

The following sections describe the boot process for network and local boot options.

Network Boot

When booting over the network using EZ-Install, Netboot, or Directed Netboot, the router essentially

1. Powers on.
2. Determines its IP address.
3. Obtains a software kernel file and/or configuration file by communicating with a configured BOOTP server on the IP network.
4. Reboots, using the newly transferred image.
5. Gets application and string files over the network as it needs them.
6. Begins bridging and routing network traffic in accordance with the configuration file.

The following sections describe in more detail the key steps in this process: obtaining an IP address and downloading the image and configuration files.

Getting an IP Address

For Netboot and Directed Netboot, you configure the IP address manually. Chapter 4 describes how to use Site Manager to configure Netboot interfaces. Chapter 5 describes how to configure the netboot interfaces using the Technician Interface.

During the EZ-Install process, the router obtains its address automatically, as described next.

1. When you power on the router, it runs a set of diagnostic tests.
2. The router sends a BOOTP request to the upstream router for an IP address and subnet mask.

Note: The upstream router must have a circuit running Bay Networks Standard Point-to-Point Protocol (PPP) using HDLC or a Frame Relay permanent virtual circuit (PVC).

The AN, ANH, or ARN issues the request through all serial ports at about the same time, even if cables are not connected to these ports. Each port successively tries the following protocols until it receives a response:

- Bay Networks Standard PPP using HDLC (high-level data link control) encapsulation
- Frame Relay Annex D
- Frame Relay Local Management Interface (LMI)
- Frame Relay Annex A

The AN, ANH, or ARN makes two attempts for each protocol over each serial interface. If one does not receive a response in approximately 4 minutes, the router boots the image and configuration file in its local file system, as described in the next section, "Local Boot."

3. The first interface on the upstream router to receive the BOOTP request responds.
4. The upstream router calculates the IP address of the AN/ANH's serial interface.

   The upstream router calculates the IP address based on its protocol configuration. See Step a if the upstream router circuit is running Bay Networks Standard or is a Frame Relay PVC in direct access mode. See Step b if it is a Frame Relay PVC in group access mode.

   a. A PVC in direct access mode or a Bay Networks Standard interface calculates the IP address by adding 1 to the IP address of the interface that received the request.

For example, in Figure 1-1 the upstream router's interface address is 192.32.1.1. This means that the upstream router calculates 192.32.1.2 as the booting router's IP interface.

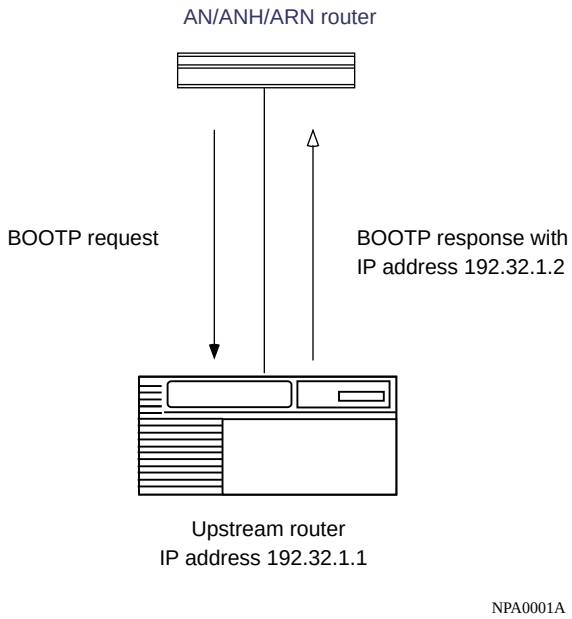

Figure 1-1. Getting an IP Address from a Bay Networks Standard Circuit or a Frame Relay PVC in Direct Access Mode

Note: If the IP address plus 1 equals a broadcast address, the upstream router calculates the IP address by subtracting 1. For example, if its interface is 7.255.255.254, the IP interface for the booting router is 7.255.255.253.

b. A PVC in group access mode references its BOOTP client interface table to find an associated IP address for the booting router.

Note: The BOOTP client interface table contains a data link connection identifier (DLCI) and IP address pair for each PVC. You use Site Manager to create this table when you follow the instructions for setting up routing paths in Chapter 4.

For example, in Figure 1-2, an AN/ANH/ARN router sends BOOTP requests for its IP address. The upstream router receives the request on PVC 31. The upstream router determines the DLCI, refers to DLCI 31 in the BOOTP client interface table, finds the IP address, and sends a BOOTP response containing the IP address back to PVC 31.

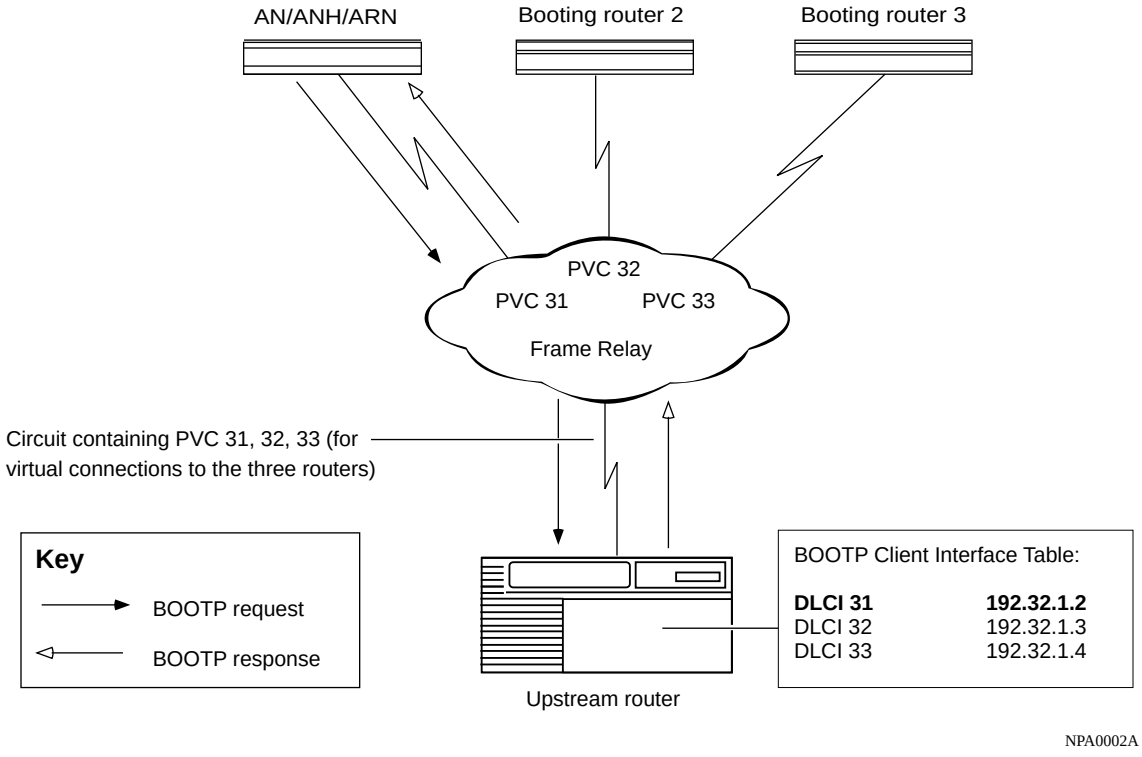

Figure 1-2. Getting an Address from a PVC in Group Access Mode

5. The upstream router sends the IP address and subnet mask to the AN/ANH/ARN in a BOOTP response message.
6. The AN/ANH/ARN assigns the IP address and subnet mask to any serial interface that receives a BOOTP response.
7. The AN/ANH/ARN stores these addresses, along with the address of the next-hop router, in RAM.

If both serial interfaces receive BOOTP responses, the AN/ANH/ARN assigns the respective IP addresses to each interface.

Getting Kernel Image and Configuration Files

With a known IP address, the AN/ANH/ARN can get image and configuration files.

1. The AN/ANH/ARN sends a BOOTP request for the pathnames of a configuration file and image kernel.

   The router issues the request simultaneously through all serial (COM), Ethernet, and Token Ring (ARN only) interfaces that have IP addresses. It issues this request periodically for about 3 minutes, regardless of whether a cable is connected.

2. A BOOTP server responds to the router's request with the directory pathnames (Figure 1-3).

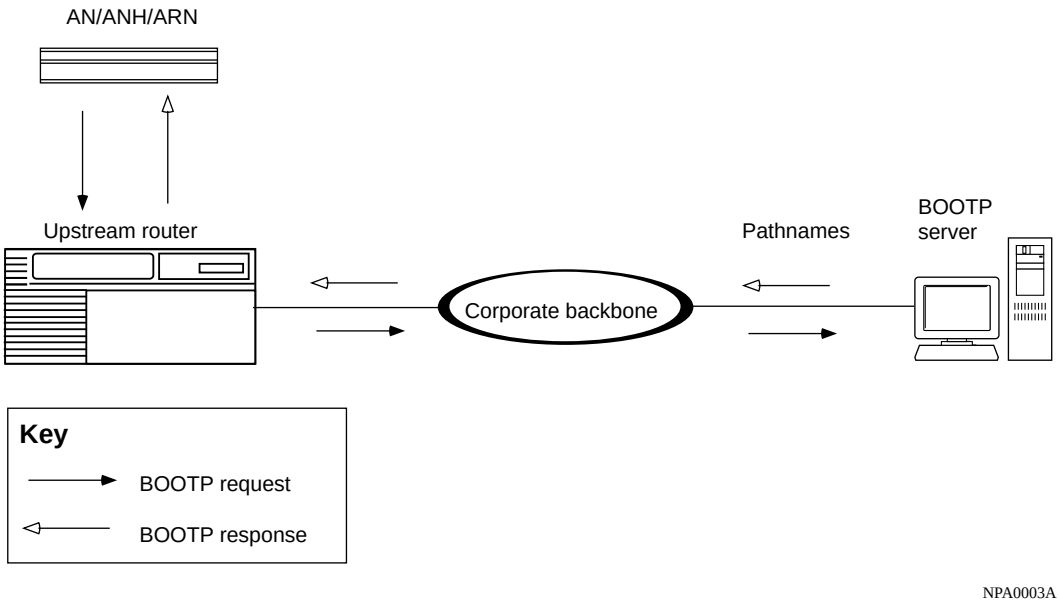

Figure 1-3. Getting the Pathnames of the Kernel and Configuration Files

The first router interface that processes the BOOTP response acts as the TFTP client in the remaining steps.

3. The AN/ANH/ARN stops sending BOOTP requests.
4. The AN/ANH/ARN sends a TFTP request for the configuration file.
5. The BOOTP server uses TFTP to transfer the configuration file (Figure 1-4).

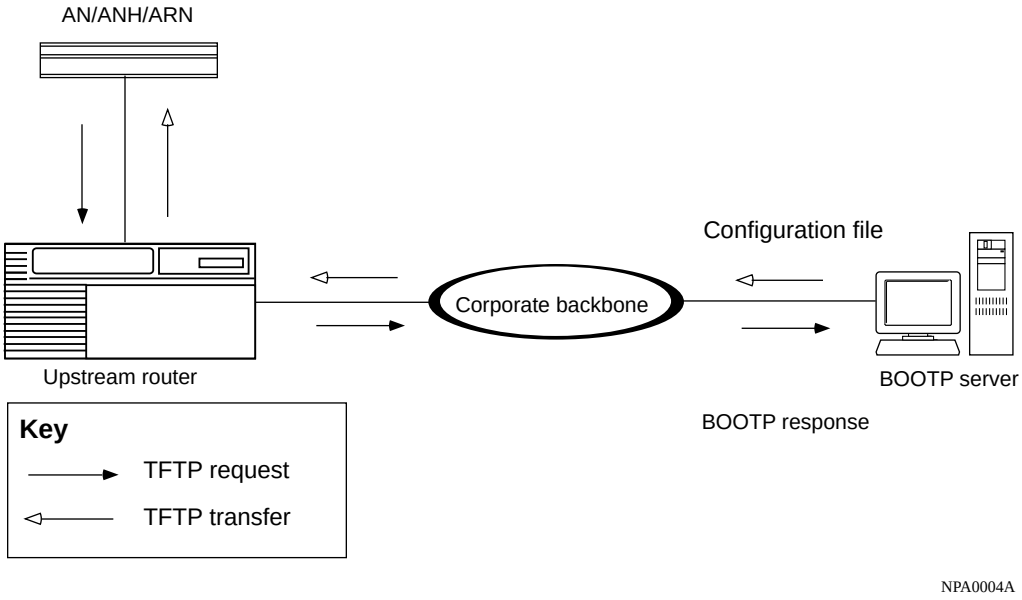

Figure 1-4. Getting the Configuration File

6. The AN/ANH/ARN sends a TFTP request for the image kernel file.
7. The BOOTP server uses TFTP to transfer the image kernel file (Figure 1-5).

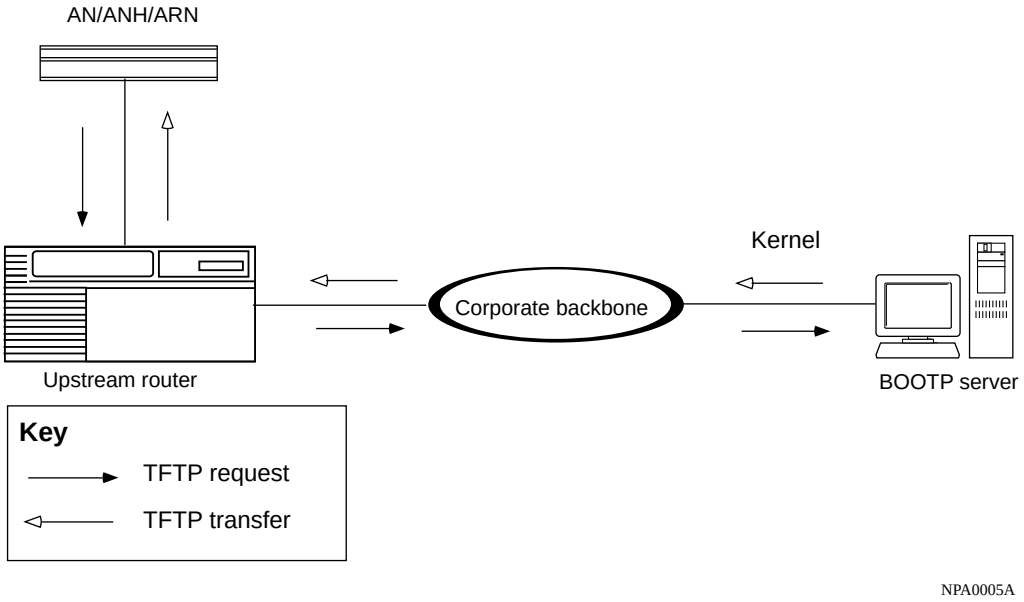

Figure 1-5. Getting the Kernel

8. The AN/ANH/ARN boots the kernel.
9. The AN/ANH/ARN uses TFTP to get application and string files as it needs them.
10. The router begins bridging and routing network traffic in accordance with the configuration file.

The AN/ANH/ARN can continue to request files, even after it begins bridging and routing traffic.

If a failure occurs in Steps 1 through 8, the router attempts to boot locally.

Local Boot

When the AN, ANH, or ARN boots locally, it reads the kernel file, application files, and string files that are embedded within a local software image file (*an.exe* for the AN/ANH or *arn.exe* for the ARN).

When you use Local Boot as the initial boot option, you boot a default (generic) configuration file. You must then run the installation script to customize the default configuration file.

Running the installation script establishes an IP network interface between the AN/ANH/ARN and a Site Manager management workstation (Figure 1-6). To make this connection, you use a Technician Interface command.

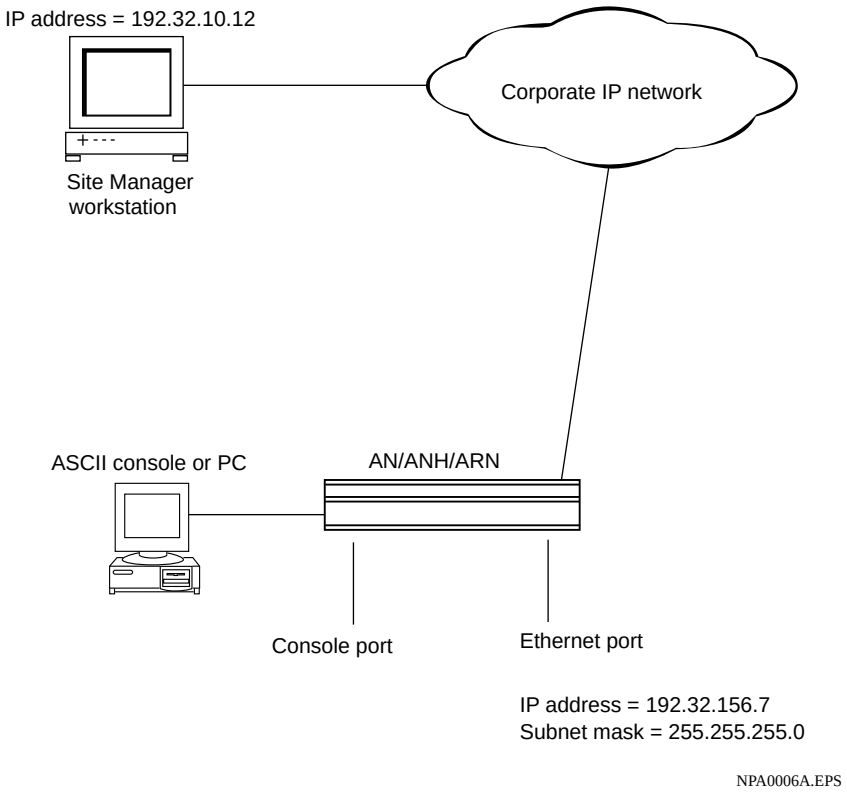

Figure 1-6. Establishing an IP Network Interface

Configuring the Initial IP Interface

Appendix B briefly describes the procedure for customizing the default configuration file, provides worksheets for preparing to run the procedure, and explains how to begin the installation script.

Chapter 2
Selecting the Boot Configuration

This chapter provides information to help you select the boot method for both the initial startup of the router and for day-to-day startup operations.

Note: To learn about the boot process and startup options, see Chapter 1.

First, refer to one of the following sections for help selecting the startup option:

- "Booting the Router for the First Time"
- "Booting the Router Routinely"

Then refer to the section, "Completing a Startup Option," for a summary of your steps.

Booting the Router for the First Time

You coordinate the initial startup with a person at the AN/ANH/ARN site, who physically installs and cables the router and initiates the desired startup procedure. The hardware installation manual (*Installing and Operating BayStack AN and ANH Systems* or *Installing and Operating BayStack ARN Routers*) explains these tasks in detail.

After you select the initial startup configuration and set up the network (as described in this guide), you instruct the person at the router site to begin the appropriate startup option.

Note: As an alternative to another person performing the initial startup at the remote site, you can perform these tasks using a modem connection.

EZ-Install

You can use EZ-Install for the initial startup if

- There is a communications link between the AN/ANH/ARN and an upstream router over an HDLC or Frame Relay interface.
- A directory on a BOOTP server contains a customized configuration file for the AN/ANH/ARN.

EZ-Install is the default option for a new router. It is the easiest option for the person at the AN/ANH/ARN site to perform, because the network automatically supplies the IP address and configuration file.

Netboot

You can use Netboot if

- The AN/ANH/ARN has a communications link to an upstream router over an Ethernet, HDLC, Frame Relay, or Token Ring (ARN only) interface.
- You establish a local console or modem connection with the AN/ANH/ARN.
- A directory on a BOOTP server contains the software image file (*krnl_an.exe* for the AN/ANH or *krnl_arn.exe* for the ARN) and a network configuration file customized for the router.
- You configure an IP address for the router's boot interface.

Netboot takes longer than EZ-Install, but minimizes the cost of line usage and the saturation of the router's memory.

Local Boot

You can use Local Boot if the router has the *an.exe* image (for the AN or ANH) or *arn.exe* image (for the ARN) on its local file system.

When you use Local Boot as the initial boot option, the router boots a default (generic) configuration file. You must then complete the installation script to customize the default configuration file and save it locally.

Refer to the information about the installation procedure and associated worksheets in Appendix B.

Recommendations

Even if you choose EZ-Install, we strongly recommend that you connect a modem or a console to the router. With a console connection, you can issue commands to the router and display messages. This is very useful if you have network problems after installing the router.

Booting the Router Routinely

This section compares the Netboot, Directed Netboot, and Local Boot options to help you choose a boot configuration for routine startups.

Note: You can boot an AN, ANH, or ARN over the network for some procedures and locally for others, provided you set up the network to support Netboot.

Netboot

Using Netboot for routine startups allows you to

- Manage software image and configuration files from a remote location by storing them on the BOOTP server.

  This option greatly simplifies the management of a number of routers by allowing you to concentrate on keeping the startup files up to date in a single, central location -- the BOOTP server.

- Minimize the need to maintain the router's local file system.

  When the router gets files from a BOOTP server, it stores the files in memory, not in its file system, reducing the need for frequent file system compactions. (Refer to *Using Technician Interface Software* or *Managing Routers and BNX Platforms* to learn about compacting a file system.)

- Restore a corrupted file system.

  The router's file system resides on an installed Flash card. With Netboot enabled, the router can still boot over the network, if the local files become corrupted. (When the router reboots due to a reset or power loss, it automatically boots the configuration file and software image over the network if it cannot find intact files locally.)

- Get application and string files from the BOOTP server as the router needs them.

  Getting these files individually, rather than getting the entire *an.exe* or *arn.exe* file, minimizes the cost of line usage and prevents saturation of the router's memory.

A disadvantage to Netboot is that it requires the most time to boot the router.

Directed Netboot

Directed Netboot requires a preconfigured communications link to a TFTP server that contains the router's boot image and a customized configuration file.

Compared with Netboot, Directed Netboot

- Creates less network traffic
- Is generally faster

Directed Netboot is usually reserved for starting the router after the initial startup because you need to know the exact location of the software image and configuration files. During Directed Netboot, the router transfers files from a TFTP server directly, bypassing negotiation with a BOOTP server for the IP address and pathname to the software files.

Local Boot

When you choose the Local Boot option for routine startups, the router reads the IP addresses from the local configuration file and assigns them to the appropriate interfaces.

Local-booting the software image and/or configuration file for routine startups allows you to

- Minimize the time it takes to boot routers.

  Typically, local-booting an image takes 2 to 3 minutes. Netbooting an image takes a little longer. For example, over a low-speed WAN or after configuring the router to run numerous protocols, Netbooting an image can take up to 15 or 20 minutes.

  It also takes less time to local-boot a configuration file than it does to Netboot one. In most configurations, however, the difference between the two options is only a few seconds.

- Minimize line usage.

  Getting files from a BOOTP server during Netboot adds traffic to your network during the booting process.

Recommendations

Bay Networks recommends that you

- Set up the network to support Netboot, even if you plan to use the Local Boot option for the initial configuration and for subsequent restarts.
- Maintain the software image (*an.exe* or *arn.exe*) on the local file system at all times, in case you want to use Local Boot for either of these routers.

Completing a Startup Option

This section lists the steps required to complete

- EZ-Install
- Netboot
- Directed Netboot
- Local Boot

You can use Netboot for some procedures and Local Boot for others, provided you set up the network to support Netboot.

Note: To boot an AN/ANH/ARN over the network, all other routers in the path to the BOOTP server must be running Router Software Version 7.60 or later.

EZ-Install

Completing the EZ-Install option requires the following steps:

1. You use the Configuration Manager in local mode to create a complete configuration file for the router. (See Chapter 4 and *Configuring Routers*.)
2. You set up a UNIX workstation on the network to support BOOTP. (See Chapter 3.)
3. You create a BOOTP relay interface table on the upstream router to support automated addressing, and configure all routers between the BOOTP server and the booting router as BOOTP relay agents. (See Chapter 3.)
4. You ensure that there is a network connection from a synchronous interface on the AN/ANH/ARN to the upstream router.

Note: If the AN/ANH/ARN will connect to the upstream router using a Frame Relay circuit, be sure that the upstream router is running Router Software Version 7.80 or later.

5. A person at the AN/ANH/ARN site installs and boots the router. (See your router hardware installation manual.)

6. The AN/ANH/ARN gets a software image from its local file system, an IP address from the upstream router, and the customized configuration file from the BOOTP server. (Chapter 1 describes this process; no action is required.)

If the configuration file meets your network requirements, the AN/ANH/ARN starts bridging and routing traffic.

You can use the Site Manager Statistics Manager and Events Manager tools to verify that the router is routing traffic according to the configuration you want. (See *Managing Routers and BNX Platforms*.)

Netboot

Completing the Netboot option requires the following steps:

1. You use the Configuration Manager in local mode to create a complete configuration file for the router. (See Chapter 4 and *Configuring Routers*.)
2. You set up a UNIX workstation on the network to support BOOTP. (See Chapter 3.)
3. You use Site Manager to enable BOOTP on each router interface in the path between the router and the BOOTP server. (See Chapter 4.)
4. You ensure that there is a network connection from a synchronous, Ethernet, or Token Ring (ARN only) interface on the AN/ANH/ARN to the upstream router.

Note: If the AN/ANH/ARN will connect to the upstream router using a Frame Relay circuit, be sure that the upstream router is running Router Software Version 7.71 or later.

5. The person at the AN/ANH/ARN site establishes a Technician Interface session, or you establish a session via modem. (See your router installation manual.)
6. The person at the AN/ANH/ARN console uses the **bconfig** and **ifconfig** commands to configure a synchronous, Ethernet, or Token Ring (ARN only) interface. (See Chapter 5 and your router installation manual.)
7. You install the *netboot.exe* file in the BOOTP server's file system, and make sure that the image and application files reside in the same directory. (See Chapter 3.)

8. The person at the AN/ANH/ARN site boots the router. (See your router hardware installation manual.)

   After the router boots, it gets the software image and configuration file from the BOOTP server.

If the configuration file meets your network requirements, the router starts bridging and routing traffic.

You can use the Site Manager Statistics Manager and Events Manager tools to verify that the router is routing traffic according to the configuration you want. (See *Managing Routers and BNX Platforms*.)

Directed Netboot

Completing the Directed Netboot option requires the following steps:

1. You use the Configuration Manager in local mode to create a complete configuration file for the router. (See Chapter 4 and *Configuring Routers*.)
2. You set up the network to support TFTP. (See Chapter 3.)
3. You ensure that there is a network connection from a synchronous, Ethernet, or Token Ring (ARN only) interface on the AN/ANH/ARN to the upstream router.

Note: If the AN/ANH/ARN will connect to the upstream router using a Frame Relay circuit, be sure that the upstream router is running Router Software Version 8.00 or later.

4. The person at the AN/ANH/ARN site establishes a Technician Interface session (or you establish a session via modem). (See your router hardware installation manual.)
5. The person at the AN/ANH/ARN console issues **bconfig** and **ifconfig** commands to configure a synchronous, Ethernet, or Token Ring (ARN only) interface for Directed Netboot. (See Chapter 5 if you are using a remote Technician Interface session or, at the router site, refer to your router installation manual.)
6. You install the *netboot.exe* file in the BOOTP server's file system, and make sure that the image and application files reside in the specified directory. (See Chapter 3.)

7. The person at the router site boots the router. (See your router installation manual.)

   The router gets the software image and configuration file from a TFTP server.

   The router starts bridging and routing traffic.

You can use the Site Manager Statistics Manager and Events Manager tools to verify that the router is routing traffic according to the configuration you want. (See *Managing Routers and BNX Platforms*.)

Local Boot

Completing the Local Boot option requires the following steps:

1. You complete the configuration worksheets. (See Appendix B.)
2. Either a person at the remote site (using a local console connection) or you (using a modem connection) establish a Technician Interface session. (See Chapter 5 and your router installation manual.)

   If you are not at the AN/ANH/ARN console, you provide the person at the remote router site with the information necessary to complete the configuration worksheets in the hardware installation manual. (See Appendix B.)
3. The person at the AN/ANH/ARN console runs the installation script (*install.bat* for the AN/ANH, *inst_arn.bat* for the ARN), using the information provided in the worksheets you completed in Step 1. (See Appendix B and your router installation manual.)
4. The installation script records the responses in a configuration file. (See Appendix B and your router installation manual.)

   The router starts bridging and routing traffic.

You can use the Site Manager Statistics Manager and Events Manager tools to verify that the router is routing traffic according to the configuration you want. (See *Managing Routers and BNX Platforms*.)

Chapter 3
Setting Up a UNIX Boot Server

To support network booting, you need to set up a UNIX workstation on the network to run BOOTP and TFTP. This chapter describes what you need to do at a UNIX workstation to prepare for booting the router over the network.

When a router boots over the network, it gets its startup files from a UNIX server. When the router uses EZ-Install or Netboot, the server supplies configuration file and/or software image file pathnames using BOOTP. The router then retrieves the files using TFTP. When the router uses Directed Netboot, it already knows the pathnames of the files it needs and retrieves the files directly from the server using TFTP.

To Configure This Boot Method	Complete These Sections
EZ-Install	"Setting Up a BOOTP Server" and "Setting Up a TFTP Server"
Netboot	"Setting Up a BOOTP Server" and "Setting Up a TFTP Server"
Directed Netboot	"Setting Up a TFTP Server"

Setting Up a BOOTP Server

To support EZ-Install or Netboot, the router needs a network connection to a BOOTP server. You configure a UNIX workstation as a BOOTP server by

- Setting up BOOTP sockets
- Configuring *BOOTPD* (the BOOTP daemon)

Note: A daemon is an unattended process (that is, one that runs in the background). An application typically calls a daemon to perform a standard routine or service (in this case, BOOTP).

On Sun workstations, you must first copy the BOOTPD program to the appropriate directory.

Copying the BOOTPD Program on Sun Workstations

Depending on the operating system you use, Bay Networks may or may not ship BOOTPD with the Site Manager package. The AIX and HP-UX operating systems already have BOOTPD. SunOS and Solaris do not, so Site Manager automatically installs BOOTPD on Sun workstations running SunOS and Solaris.

Copy the *bootpd* file to the */etc* directory as follows:

1. **Log in to the UNIX workstation as *root*.**
2. **Enter the following command:**

   cp /usr/wf/bin/bootpd /etc

Setting Up BOOTP Sockets

A *socket* is a UNIX mechanism for creating virtual connections between operating system and network processes. For each socket, the */etc/services* file must include a User Datagram Protocol (UDP) descriptor that provides process-to-process addressing information.

Set up the send and receive sockets for the BOOTP process as follows:

1. **Log in to the UNIX workstation as *root*.**

2. **Use a text editor to insert the following two lines into the** */etc/services* **file:**

```
bootps          67/udp          # bootp server
bootpc          68/udp          # bootp client
```

Setting Up BOOTPD to Run

Configure your workstation to run the BOOTPD program when it receives a BOOTP request packet, as follows:

1. **As** *root***, use a text editor to open the** */etc/inetd.conf* **file.**
2. **Make sure that no other line in the file begins with "bootps."**

   If there is such a line, your workstation is already configured as a BOOTP server. Comment out this line by entering a pound sign (#) at the beginning of the line, so that the server will use the BOOTPD program that you specify in the next step.
3. **Insert the following line anywhere in the file to configure your workstation as a BOOTP server:**

   ```
   bootps dgram udp wait root /etc/bootpd bootpd
   ```
4. **Save and exit the file.**

Setting Up BOOTPD to Respond to Routers

When the operating system receives a BOOTP packet, it starts up BOOTPD. The BOOTPD software matches the source IP address of the packet to an IP address in its BOOTP table (*bootptab*) file to determine the pathnames to configuration and boot image files.

Note: The *bootptab* file can include the same boot image pathname for all booting routers, or a different boot image for each IP address.

Entries in *bootptab* also include optional parameter tags. Bay Networks supplies a sample *bootptab* file that Site Manager installs automatically in the */usr/wf/config* directory. Use a copy of this sample file if you do not already have a *bootptab* file.

Set up BOOTPD to respond to booting routers, as follows:

1. **As *root*, view the contents of the */etc* directory to determine whether it already contains a *bootptab* file.**

   If it does contain a *bootptab* file, disregard Steps 2 and 3 and continue with Step 4 to edit this file.

2. **Issue the following command to copy the *bootptab* file to the */etc* directory:**

   cp /usr/wf/config/bootptab /etc

3. **Use an editor to open the *bootptab* file in the */etc* directory.**

4. **Type the information that pertains to the ANs and ANHs in your network into the *bootptab* file.**

   The section that follows explains how to format your entries. Use Tables 3-1 and 3-2 to determine which tags and values you need. Figure 3-1 shows the sample *bootptab* file included with the Site Manager software. The comments in this file explain the sample definitions.

5. **After editing the *bootptab* file, be sure to save the changes.**

Note: Be sure the bootptab file resides in the */etc* directory. BOOTPD fails if it cannot find the *bootptab* file in */etc*.

Editing the bootptab File

Enter a *<hostname>* definition in the *bootptab* file for each AN/ANH in your network. The format of each definition in the *bootptab* file is as follows:

```
<hostname>:\
:<tg>=<value>:\
:<tg>=<value>:\
:<tg>=<value>:
```

- *<hostname>* is a name you assign to a BOOTP client (each router is a client).
- *<tg>* is a BOOTP parameter name (tag).
- Follow each tag with an equal sign (=) and a value.
- A pound sign (#) at the beginning of a line indicates a comment.
- A backslash (\) at the end of a line indicates continuation of the line.

Note: Make sure you enter a backslash (\), not a slash (/), at the end of every line that does not conclude a definition.

Keep the following in mind when editing *bootptab*:

- The <*hostname*> definition can contain a maximum of 79 characters.
- The first character must be alphabetic.
- All characters must be alphanumeric.
- You can use a dot (.) to separate characters, but the character immediately following the dot must be alphabetic.
- The hostname definition cannot contain an underscore.

Table 3-1 lists the tags for router hostnames. Table 3-2 lists the tags for boot image names.

Table 3-1. BOOTPD Tags for a Router Hostname

Tag	Required or Optional	Value	Example
ip	Required	IP address -- the host IP address of the router.	ip=192.32.5.2
sm	Optional	Subnet mask -- the host subnet mask of the router.	sm=255.255.255.0
T129	Required	Pathname of the router configuration file. The maximum path length is 49 characters.	T129="/usr/cfg/an_Bost.cfg "

(continued)

Table 3-1. BOOTPD Tags for a Router Hostname *(continued)*

Tag	Required or Optional	Value	Example
T130	Required	Size of the router configuration file in 512-byte blocks. The setting of this tag determines how much memory the router allocates for the file. Set this tag to 0x0004.	T130=0x0004
tc	Optional	Table continuation -- pointer to a definition in another location in the same file for additional information. The information this tag points to is common to all routers that need to boot using BOOTP. If information in a definition for a specific router is inconsistent with the definition this tag points to, BOOTPD uses the information for the specific router.	tc=general

Table 3-2. BOOTPD Tags for a Boot Image Name

Tag	Required or Optional	Value	Example
hd	Required	Home directory -- the directory on the workstation containing the boot files. By default, the Image Builder writes its files to the directory specified in the example. The `rel...` number is the version number of the current router software release. If you change the default or move the files to another directory, specify that directory.	hd=/$HOME/.builder_dir/rel812/an
bf	Required	Boot file -- the name of the boot image.	bf=krnl_an.exe

(continued)

Table 3-2. BOOTPD Tags for a Boot Image Name *(continued)*

Tag	Required or Optional	Value	Example
bs	Required	Boot size -- the size of the boot file in 512-octet blocks. If you specify **auto** as the size, the BOOTP server calculates the size of the file for each BOOTP request.	bs=auto
vm	Required	Vendor magic cookie selector -- the BOOTP server should always reply in a manner compliant with RFC 1048. You must enter **rfc1048** for this tag, so that the router can understand the BOOTP responses it receives.	vm=rfc1048

The sample *bootptab* file in Figure 3-1 enables two ANs (named “AN.Boston” and “AN.Chicago”) to boot across the network. Use the basic format shown in Figure 3-1 to set up your own *bootptab* file.

```
# This file contains the default specification for the boot
# image file to be used by all ANs.

# "general" contains information that is common to all ANs
# that need to boot via BOOTP. You can use any word in place
# of "general."
    general:\

# "hd" specifies that /$HOME/.builder_dir/rel900/an is the
# directory on the workstation where the boot files are
# located. By default, the Image Builder writes its files to
# this directory. If you are using a router software version
# later than 8.00, add the associated three digits to the end
# of the "rel" directory name. If you moved the files to
# another directory, specify that directory.
    :hd=/$HOME/.builder_dir/rel812/an:\

# "bf" specifies that the name of the boot image kernel file
# is krnl_an.exe.
    :bf=krnl_an.exe:\

# "bs" indicates the size of the boot file. If you specify
# "auto" as the size, the BOOTP server calculates the size of
# the file for each BOOTP request.
    :bs=auto:\

# "vm" indicates that the BOOTP server should always reply in
# a manner compliant with RFC 1048. You must enter rfc1048
# for this tag so that the AN can understand the BOOTP
# responses it receives.
    :vm=rfc1048:

# This line marks the beginning of the active definition for
# the AN we are naming "AN.Boston."
    AN.Boston:\

# "ip" indicates the IP address of the AN.
    :ip=192.32.5.2:\

# "T130" indicates the size of the AN's configuration file in
# 512-byte blocks. Always use 0x0004.
    :T130=0x0004:\
# "T129" indicates the pathname of the configuration file
# for the AN.
    :T129="/usr1/cfg/AN_Bost.cfg":\

# "tc" indicates that the "general" definition contains more
# information that applies to BOOTP transmissions to
# "AN.Boston."
    :tc=general:

# This is the active definition for the AN we are naming
# "AN.Chicago."
    AN.Chicago:\
    :ip=10.0.0.4:\
    :T130=0x0004:\
    :T129="/rte3/cfg/AN_Chic.cfg":\
    :tc=general:
```

Figure 3-1. Sample bootptab File

Verifying Consistent BOOTP Service

You may want to configure a second workstation as a BOOTP server for backup purposes. If you do so, make sure that the two *bootptab* files match exactly. Also, make sure that the image and string files are from the same software version.

Setting Up a TFTP Server

An AN/ANH/ARN needs a network connection to a TFTP server to complete EZ-Install, Netboot, or Directed Netboot. You configure a UNIX workstation as a TFTP server by

- Setting up *TFTPD* (the TFTP daemon)
- Adding a TFTP user (for an HP 9000 only)
- Setting up static routes to routers (optional)
- Loading the changes into memory

Note: A daemon is an unattended process (that is, one that runs in the background). An application typically calls a daemon to perform a standard routine or service (in this case, TFTP).

When you set up the TFTPD server on a UNIX workstation, you can allow TFTP to access the root directory and any subdirectory, or restrict its access to a specified directory or pathname.

Allowing the router to access the root directory and any subdirectory is the simpler procedure. Specifying a pathname provides security, but it requires linking TFTPD.

Providing TFTPD Access to the Root Directory

To provide TFTPD access to files in the *root* directory and to all subdirectories, verify or insert the appropriate line for your operating system in the */etc/inetd.conf* file.

Find the sample line for your operating system in Table 3-3.

Table 3-3. Providing TFTPD Access to Root and All Subdirectories

Operating System (OS)	Sample Line to Insert in /etc/inetd.conf Directory
SunOS	`tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -s /`
Solaris	`tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /`
HP-UX	`tftp dgram udp wait root /etc/tftp tftp`
AIX	Use the System Management Interface Tool (SMIT) to configure TFTP. For instructions, refer to the IBM guides on TCP/IP daemons and the TFTP protocol.

Restricting TFTPD Access to a Specified Directory

To restrict TFTPD file access to a specific directory, insert the appropriate line for your operating system in the */etc/inetd.conf* file.

The examples in Table 3-4 restrict access to the */tftpboot* directory. You can substitute any directory you want.

Table 3-4. Restricting TFTPD Access to One Directory

OS	Sample Line to Insert in /etc/inetd.conf Directory
SunOS	`tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -s /tftpboot`
Solaris	`tftp dgram udp wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot`
HP-UX	`tftp dgram udp wait root /etc/tftp tftp -s /tftpboot`
AIX	Use the System Management Interface Tool (SMIT) to configure TFTP. For instructions, refer to the IBM guides on TCP/IP daemons and the TFTP protocol.

You must create a symbolic link for every pathname you specify. For example, to set up the symbolic links for the */tftpboot* path, use the following procedure:

1. **Log in to your UNIX workstation as** *root***.**

2. **Enter the following commands:**

```
cd  tftpboot
ln  -s  .  usr
ln  -s  .  tftpboot
```

Caution: Do not insert a slash (/) in the **cd tftpboot** command; a symbolic link cannot contain references to directories above the directory specified in the **tftpd** command line. Use the **-s** flag to provide additional security to your network. (This flag restricts TFTPD access to a specified directory.)

Adding a TFTP User for an HP 9000

Follow the instructions in this section only if you are using an HP 9000 as the Site Manager workstation.

To add a TFTP user for the HP 9000, enter a line with the following syntax in your */etc/passwd* file. We recommend that you use *root* (/) as the TFTP home directory.

tftp::*<user_id>***:***<group_no.>***::/:/bin/false**

For example:

```
tftp::510:20::/:/bin/false
```

Note: We recommend that you do not use the System Administration Manager (SAM) utility as an alternative to entering the commands above.

Setting Up Static Routes to Next-Hop Routers

If your workstation requires static routes, use this section to specify a path to the network by

- Editing the *inetd.conf* file
- Verifying the routes
- Loading the changes into memory

You must set up a static route for each path between the routers and the BOOTP server's next-hop router.

You may want to specify a static route in a multihop environment or in an environment using routing protocols such as RIP, where minor routing update delays may extend the time it takes to Netboot.

Editing the inetd.conf File

Add the following line to the *inetd.conf* file to set up a static route:

route add *<destination> <gateway> <hops>*

<*destination*> is the IP address of the AN/ANH or its network.

<*gateway*> is the IP address of the network destination to which packets are to be addressed.

<*hops*> is the number of hops to the network destination.

Verifying the Routes

After adding a static route for each path to the booting routers, enter the following command to display the routing table and verify the route you added:

netstat -r

Loading the Changes into Memory

Once you modify the *inetd.conf* file, you must force the operating system to reread it by rebooting the workstation or by issuing a hang-up signal.

In most cases, reboot the workstation. Issue a hang-up signal if the workstation is performing a task that you do not want to interrupt.

Rebooting

Reboot your workstation as follows:

1. **Log in as** *root***.**
2. **Enter the following command:**

   /etc/shutdown now -r

   The **-r** flag reboots the workstation.

Issuing a Hang-Up Signal

Issue a hang-up signal as follows:

1. **Log in as** *root***.**
2. **Enter the following command to hang up on the** *inetd* **process:**

   ps -aux | grep inetd

   The system displays a line similar to this one:

   ```
   root   148  0.0  0.0   48    0 ?  IW Sept 14  0:07 inetd
   ```

3. **Enter the following command, using the first number in the line after the word "root" (in this case, 148):**

   kill -1 148

The *inetd* process rereads the *inetd.conf* file.

What to Do Next

Before you can use the network to boot a remote AN, ANH, or ARN, you must also complete the steps in Chapter 4.

Chapter 4
Configuring Network Booting

This chapter describes how to use Site Manager to configure network booting for AN, ANH, or ARN routers in the network.You can also use Technician Interface commands to configure network booting, as described in Chapter 5.

Note: Before the router can get files over the network, you must also set up a UNIX BOOTP server on the network, as described in Chapter 3.

The following sections of this chapter explain how to complete the tasks required for configuring EZ-Install, Netboot, or Directed Netboot.

To Configure This Boot Method	Complete These Sections of this Chapter
EZ-Install	Preparing Configuration and Image Files
EZ-Install over Frame Relay group-access PVC	• Preparing Configuration and Image Files • Creating the BOOTP Client Interface Table
Netboot	• Enabling Netboot or Directed Netboot from Site Manager • Configuring a Netboot or Directed Netboot Interface • Setting Up Routing Paths for Netboot
Directed Netboot	• Enabling Netboot or Directed Netboot from Site Manager • Configuring a Netboot or Directed Netboot Interface

Note: The steps in this chapter assume that the Site Manager software is running on a network workstation.

Preparing Configuration and Image Files

Unless the router will use the default (generic) configuration file and software image that ships on its local Flash memory card, you must create

- A unique configuration file for each remote router
- A uniform software image that all routers in your network can use

Creating Configuration Files

Prepare network configuration files as follows:

1. **Use the Configuration Manager in local mode to create a configuration file for each AN/ANH/ARN.**

   Refer to *Configuring Routers* for instructions. Also, refer to

   - Table 4-1 for the Site Manager module name to use when creating a configuration file for BayStack AN routers
   - Table 4-2 for the module name to use when creating a configuration file for BayStack ANH systems
   - Tables 4-3 through 4-5 for the module names to use when creating a configuration file for BayStack ARN routers.

2. **Record the name of each configuration file and corresponding AN/ANH/ARN for later reference when configuring network boot options.**

   When you name configuration files, keep the following restrictions in mind:

   - Bay Networks recommends that the operational configuration file for each router be named *config*. If a router experiences a power failure, it boots from the file called *config* once power returns. However, the configuration files that you save on a BOOTP server for Directed Netboot do *not* have to be named *config* because you specify the configuration file pathname (refer to the Site Manager parameter "Boot Config Pathname.")
   - Configuration filenames must begin with an alphabetical character. The remaining characters must be alphanumeric and may also include the underscore (_) character. You cannot use spaces.

- Configuration filenames can consist of 1 to 15 characters, including a dot (period). We recommend that you limit filenames to eight characters to ensure that all operating systems that Bay Networks supports can recognize the names.
- Configuration filename extensions are optional and must follow a filename and a dot. We recommend that you limit filename extensions to three characters.
- BOOTP allows a maximum number of 49 characters in a filename path, including slashes, filename, optional dot, and filename extension.

3. **If the BOOTP server and Site Manager do not reside on the same workstation, transfer the configuration files to the BOOTP server.**

Table 4-1. BayStack AN Configurations

Base AN Interface Configuration	Upgrade Components	Site Manager Module Name
1 Ethernet (XCVR1) and 2 synchronous (COM1 and COM2)	none	E/2S
	1 ISDN BRI (replaces COM2)	E/2S/BRI
	1 ISDN BRI with Floating B channel	E/2S/BRI+
	1 Ethernet DCM	E/2S/N11 DCM
	1 third synchronous interface	E/3S
	1 second Ethernet interface	2E/2S
	1 third synchronous interface and 1 Ethernet DCM	E/3S/N11 DCM
	1 ISDN BRI with Floating B channel and 1 Ethernet DCM	E/2S/BRI+/N11 DCM
	1 second Ethernet interface and 1 Ethernet DCM	2E/2S/N11 DCM
1 Token Ring (TOKEN1) and 2 synchronous (COM1 and COM2)	none	T/2S
	1 ISDN BRI (replaces COM2)	T/2S/BRI
	1 ISDN BRI with Floating B channel	T/2S/BRI+
	1 third synchronous interface	T/3S

(continued)

Table 4-1. BayStack AN Configurations *(continued)*

Base AN Interface Configuration	Upgrade Components	Site Manager Module Name
1 Ethernet (XCVR1), 1 Token Ring (TOKEN1), and 2 synchronous (COM1 and COM2)	none	E/T/2S
	1 ISDN BRI (replaces COM2)	E/T/2S/BRI
	1 third synchronous interface	E/T/3S
	1 ISDN BRI with Floating B channel	E/T/2S/BRI+
	1 Ethernet DCM	E/T/2S/N11 DCM
	1 ISDN BRI with Floating B channel and 1 Ethernet DCM	E/T/2S/BRI+/N11 DCM
	1 third synchronous interface and 1 Ethernet DCM	E/T/3S/N11 DCM

Table 4-2. BayStack ANH Configurations

Model	Base Interface Configuration	Added Components	Site Manager Module Name
8-port ANH	1 Ethernet repeater (XCVR1) and 2 synchronous (COM1 and COM2)	none	8pt EHub/2S
		1 Ethernet DCM	8pt EHub/2S/N11 DCM
		1 third synchronous interface (COM3)	8pt EHub/3S
		1 second Ethernet interface (XCVR2)	8pt EHub/E/2S
		1 ISDN BRI with Floating B channel	8pt EHub/2S/BRI+
		1 third synchronous interface and 1 Ethernet DCM	8pt EHub/3S/N11 DCM
		1 second Ethernet interface and 1 Ethernet DCM	8pt EHub/E/2S/N11 DCM
		1 ISDN BRI, 1 Ethernet DCM	8pt EHub/2S/BRI+/N11 DCM
12-port ANH	1 Ethernet repeater (XCVR1) and 2 synchronous (COM1 and COM2)	none	12Pt EHub/2S
		1 ISDN BRI (replaces COM2)	12Pt EHub/2S/BRI
		1 third synchronous interface	12Pt EHub/3S
		1 second Ethernet interface	12Pt EHub/E/2S
		1 ISDN BRI with Floating B channel	12Pt EHub/2S/BRI+

Table 4-3 lists the *base modules* (system boards) for BayStack ARN systems. An ARN can have only one base module.

Table 4-3. BayStack ARN Base Module Configurations

Base Module	Site Manager Module Name
Ethernet	Ethernet
Ethernet with DCM	Ethernet/DCM
Token Ring	Token Ring

Table 4-4 lists the optional *expansion modules* available for an ARN. An expansion module is a parallel daughterboard installed on the base module. The ARN base module supports one expansion module only.

Table 4-4. BayStack ARN Expansion Module Configurations

Expansion Module	Site Manager Module Name
Ethernet	Ethernet
Ethernet with DCM	Ethernet/DCM
Token Ring	Token Ring
Tri-Serial	TRI Serial
Ethernet/Tri-Serial	Ethernet/TRI Serial
Ethernet/Tri-Serial with DCM	Ethernet/TRI Serial/DCM
Token Ring/Tri-Serial	Token Ring/TRI Serial

Table 4-5 lists the available adapter modules for an ARN. An adapter module is a serial daughterboard installed in the front panel card cage. The ARN base module supports one or two adapter modules.

Table 4-5. BayStack ARN Adapter Module Configurations

Adapter Module	Site Manager Module Name
Serial	Serial
ISDN BRI S/T	ISDN ‘S/T’
ISDN BRI U	ISDN ‘U’

(continued)

Table 4-5. BayStack ARN Adapter Module Configurations *(continued)*

Adapter Module	Site Manager Module Name
56/64K DSU/CSU	56/64K DSU/CSU
V.34 Modem	V34 Modem

Preparing an Image

If you want the router to automatically boot a network-based image when starting up (using Netboot or Directed Netboot), use the Site Manager Image Builder to create the kernel, application, and string files for storage on the BOOTP/TFTP server. To use Image Builder:

1. **On the Site Manager workstation, open the software image file in the Image Builder.**

   Keep the following in mind:

   - Be sure to select the correct image (*an.exe* for an AN or ANH, or *arn.exe* for an ARN). If you select an image for another router type, you cannot generate the correct files.
   - If you configure the router to obtain its image from the network, it cannot Netboot the image until the kernel image is available on the BOOTP server.
   - Make sure that you extract the kernel image and all of the application (*.exe*) files and string (*.str*) files in the router directory. The files must be from the same software image file whose components were created from the same version of software. If these files are from different software versions, the router may fail to boot or may not operate properly.

   After you open the image file, the Image Builder automatically generates the kernel image, application files, and AN/ANH/ARN string files.

   By default, the Image Builder stores these files in */$HOME/.builder_dir/rel<rel>/an* (for the AN and ANH) and */$HOME/.builder_dir/rel<rel>/arn* (for the ARN). In the pathname, *<rel>* is the current router software release for the router). For example, Version 2.12 of the Site Manager Image Builder tool stores Version 8.12 files for an AN or ANH in the */$HOME/.builder_dir/rel812/an* directory.

   For additional instructions on how to use the Image Builder, refer to *Modifying Software Images for Routers.*

2. **If you use a different workstation as a BOOTP server, transfer to the new workstation all of the files in the directory that contains the kernel file.**

Enabling Netboot or Directed Netboot from Site Manager

By default, the router obtains its software image from its local file system and its configuration file from a BOOTP server. Display and change these settings as follows:

1. **Select Protocols > Global Protocols > Net Boot > Global from the Configuration Manager window.**

   The Edit Netboot Global Parameters window appears (Figure 4-1).

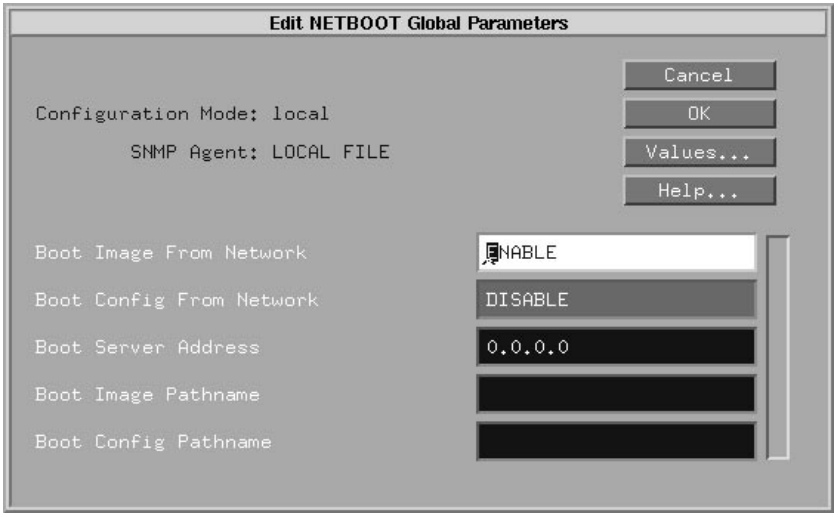

Figure 4-1. Edit Netboot Global Parameters Window

2. **To enable Netboot, set one or both of the first two parameters to "Enable."**

3. **To enable Directed Netboot, set one or both of the first two parameters to "Enable" and configure the last three parameters.**

   For guidelines, see the descriptions of the parameters that follow this procedure.

4. **After editing the parameters, click on OK.**

Note: Of the five parameter fields shown in Figure 4-1, the first two (Boot Image From Network and Boot Config From Network) apply to both Netboot and Directed Netboot. The last three parameters are for Directed Netboot only.

Netboot and Directed Netboot Parameters

Parameter: **Boot Image From Network**

Default: Disable

Options: Enable | Disable

Function: Enables or disables retrieval of the software image from the BOOTP server the next time the router starts up.

Instructions: Set to Disable if you want to boot using the image in the router's local file system. This setting reduces the time it takes to boot the router and eliminates using network resources to obtain the image.

Set to Enable if

- You want the router to obtain the image from a BOOTP server and you have already set up the network to support BOOTP service.
- You are upgrading the image on a number of routers. The routers can then boot using a single image on the BOOTP server. You must ensure that the directory name in the *bootptab* file matches the location of the upgraded image before you boot the routers.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.10.1.1

Note: Instead of enabling the Boot Image From Network parameter, you can use the Router Files Manager to transfer an upgraded image to the AN/ANH/ARN. To do this, delete the old software image file, compact the file system, and copy the upgraded image file to the AN/ANH/ARN. Use the Router Files Manager to confirm that the upgraded image on the router is the same size as that on the Site Manager workstation. This verifies that the file transfer was successful. Refer to Managing Routers for more information on the Router Files Manager.

Parameter:	**Boot Config From Network**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables retrieval of the configuration file from a BOOTP server the next time the router starts up.
Instructions:	Set to Disable if you have already saved the configuration file in the router's memory to the router's file system, and you want to boot using this configuration file. This setting reduces the time it takes to boot the router and eliminates using network resources to obtain the configuration file. Set to Enable if you want the router to obtain the configuration file from a BOOTP server and you have already set up the network to support BOOTP service.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.1.2

Parameter:	**Boot Server Address**
Default:	None
Options:	A valid IP address of a TFTP server
Function:	When one or both of the parameters Boot Image From Network and Boot Config From Network are set to Enable, this parameter specifies the TFTP server from which the router will obtain the boot image and boot configuration files.
Instructions:	Use this parameter only when configuring Directed Netboot. Enter the valid IP address of the TFTP server, in dotted decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.1.3

Parameter:	**Boot Image Pathname**
Default:	None
Options:	A valid image file pathname
Function:	When the parameter Boot Image From Network is set to Enable, this parameter specifies the absolute pathname of the boot image file on the TFTP server.
Instructions:	Use this parameter only when configuring Directed Netboot. Make sure that the file you specify is the valid image file on the TFTP server.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.1.4

Note: When you Netboot a router, the active image parameter shows the full path to the active image on the remote server. When you boot an AN/ANH/ARN locally, the name of the active image (wfHwEntry.wfHwActiveImageName) appears in the form <volume>:<image name>.

Parameter:	**Boot Config Pathname**
Default:	None
Options:	A valid configuration file pathname
Function:	When the parameter Boot Config From Network is set to Enable, this parameter specifies the absolute pathname of the boot configuration file on the TFTP server.
Instructions:	Use this parameter only when configuring Directed Netboot. Make sure that the file you specify is the valid configuration file on the TFTP server.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.1.5

Configuring a Netboot or Directed Netboot Interface

When you enable Netboot or Directed Netboot, you must configure at least one AN/ANH/ARN circuit as a Netboot interface. If you are using EZ-Install, you do not need to configure Netboot interfaces.

To add a Netboot interface from Site Manager:

1. **Select Protocols > Global Protocols > Net Boot > Interfaces from the Configuration Manager window.**

   The Netboot Interfaces window appears (Figure 4-2).

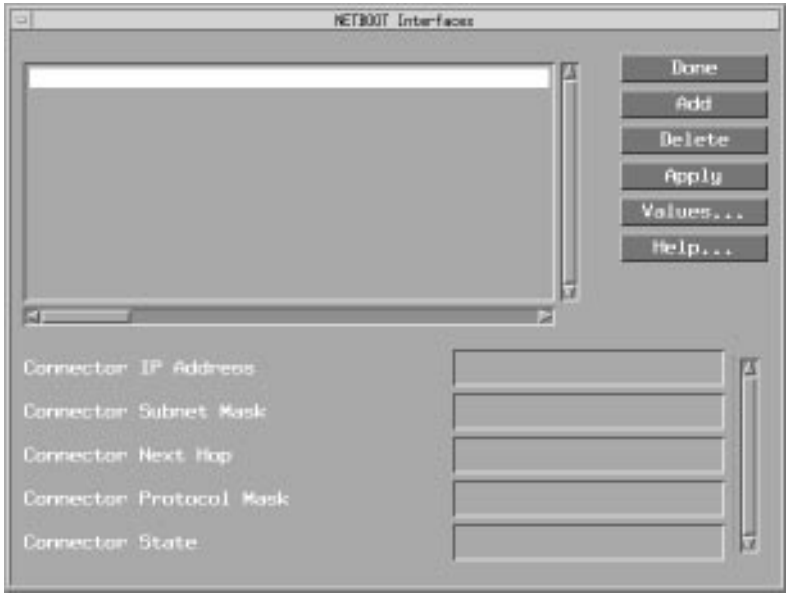

Figure 4-2. Netboot Interfaces Window

   The scroll box is empty unless this router has existing Netboot interfaces configured.

2. **Click on Add.**

   The Netboot Interface window appears (Figure 4-3).

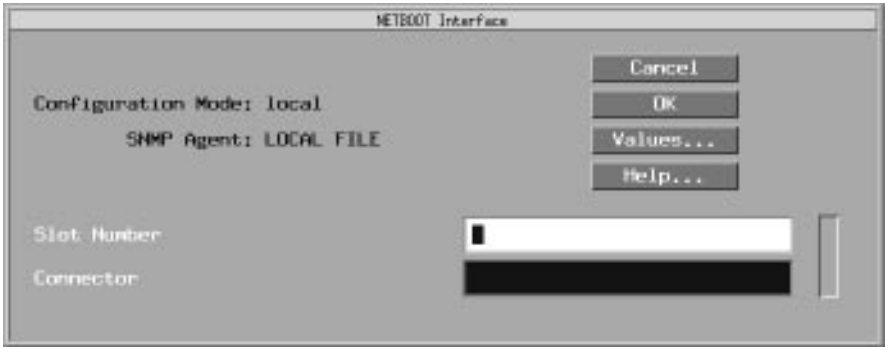

Figure 4-3. Netboot Interface Window

3. **Specify Slot Number 1 as the physical slot in which the hardware module is installed.**

   Be sure that number 1 appears in the Slot Number box. (AN, ANH, and ARN systems have only one slot.)

4. **Enter the name of the connector configured for the Netboot interface.**

   Enter COM1, COM2, COM3, COM4, or COM5 to configure Netboot over a synchronous interface.

   Enter XCVR1 or XCVR2 to configure Netboot over an Ethernet interface.

   Enter TOKEN1 or TOKEN2 to configure Netboot over a Token Ring interface (ARN only).

   Note that the interfaces that are available to you depend on the interface options you purchased with your router.

5. **Click on OK.**

   The Netboot Interfaces window now shows the configured interface (Figure 4-4).

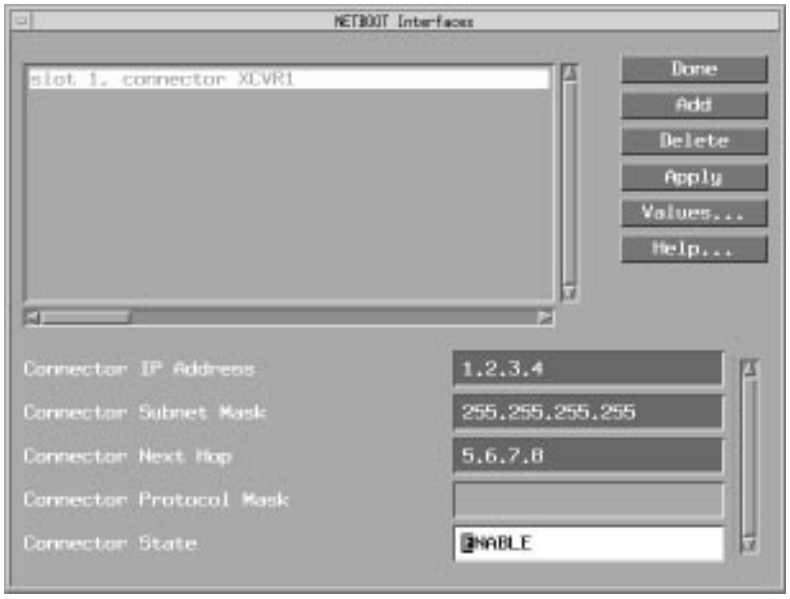

Figure 4-4. Netboot Interfaces Window

6. **Highlight the interface in the scroll box and edit its parameters.**

   For guidelines, see the parameter descriptions that follow this procedure.

7. **Click on Apply.**

8. **Repeat Steps 2 through 7 to add any additional Netboot interfaces that you want to configure.**

Note: If you configure more than one interface to Netboot, the first interface to receive a reply from the BOOTP server will use Netboot to reach the router.

9. **Click on Done to exit the Netboot Interfaces window.**

Netboot Interface Parameters

Parameter:	**Connector IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP address of this interface.
Instructions:	Enter the IP address of this interface in dotted decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.3.1.4

Parameter:	**Connector Subnet Mask**
Default:	None
Options:	Any valid IP subnet mask
Function:	Specifies the network and subnetwork portion of the 32-bit IP address of this interface. The Configuration Manager automatically calculates an appropriate subnet mask, depending on the class of the network to which the interface connects. However, you can change the subnet mask with this parameter.
Instructions:	Accept the assigned subnet mask, or enter one in dotted decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.3.1.5

Parameter:	**Connector Next Hop**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP address of the next-hop router connected to this interface. When the router starts up, the next-hop router passes the BOOTP requests and responses that initiate the transfer of the image and/or configuration file between the router and the BOOTP server. If the router and BOOTP server are on the same IP subnet, you do not have to set this parameter.
Instructions:	Enter the IP address of the next-hop router connected to the interface you are adding, in dotted decimal notation.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.3.1.6

Parameter:	**Connector Protocol Mask**
Default:	Point to Point
Options:	Point to Point | Point to Point Internal Clock | Fr Relay Annexd | Fr Relay Annexa | Fr Relay LMI
Function:	During the boot process, the router will configure the synchronous interface to the specified protocol.
Instructions:	Specify the desired protocol option.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.3.1.7

Parameter:	**Connector State**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables Netboot on this interface. When set to Enable, any settings already entered in the other four parameter boxes in the Netboot Interfaces window appear and are noted by Site Manager so that Netboot occurs. If the setting is Disable, Site Manager disregards the other parameters and the router cannot Netboot.
Instructions:	If you do not want Site Manager to use the settings on the Netboot Interfaces window, set this parameter to Disable. If you want Site Manager to use any of the other four parameters in the Netboot Interfaces window (refer to Figure 4-2), you must set this parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.10.3.1.1

Setting Up Routing Paths for Netboot

You set up the routing paths between the BOOTP server and the routers by

- Enabling each router interface in the paths to the routers
- Creating a BOOTP relay agent forwarding table for each router in the path
- Creating a BOOTP client interface table for the upstream router when the AN/ANH/ARN is on a Frame Relay PVC in group access mode

Enabling Router Interfaces

You must enable BOOTP relay (also called BOOTP pass-through or gateway) on all interfaces in the paths between the AN/ANH/ARN routers and the BOOTP server. For example, you would enable BOOTP relay on the interfaces indicated in Figure 4-5.

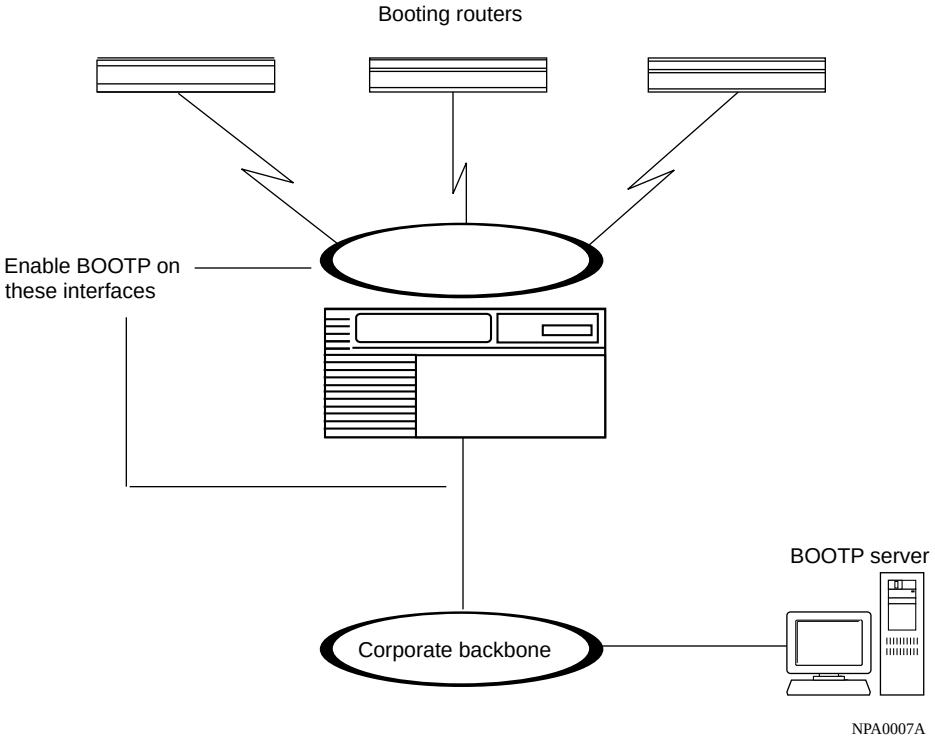

Figure 4-5. Enabling BOOTP in a Sample Network

Enable BOOTP relay on an interface as follows:

1. **Click on the connector in the Configuration Manager window.**
2. **Select Edit Circuit in the Edit Connector window.**
3. **Select Protocols > Add in the Circuit Definition window.**
4. **Select BOOTP in the Select Protocols window and click on OK.**
5. **Select File > Exit to exit the Circuit Definition window.**

Creating BOOTP Relay Agent Forwarding Tables

You must create a BOOTP relay agent forwarding table for every router passing BOOTP traffic between the router and the BOOTP server.

The BOOTP relay agent forwarding table allows you to specify the IP interface that receives the incoming BOOTP request packets, and the associated IP interface that forwards them. You can add multiple pairs of incoming and outgoing interfaces to support connections to multiple routers in your network.

To create the BOOTP relay agent forwarding table, begin at the Configuration Manager window and complete the following steps.

1. **Select Protocols > IP > BOOTP > Relay Agent Interface Table.**

   The BOOTP Relay Agent Interface Table window appears (Figure 4-6). This window lists all IP interfaces on the router.

Figure 4-6. BOOTP Relay Agent Interface Table Window

Click on Help or refer to *Configuring SNMP, BOOTP, DHCP, and RARP Services* for a description of the parameters in the BOOTP Relay Agent Interface Table window.

Note: Be sure that the Timeout Secs. parameter is set to the default, 0.

2. **Click on Forward I/F (interface).**

   The BOOTP Relay Agent Forwarding Table window appears (Figure 4-7).

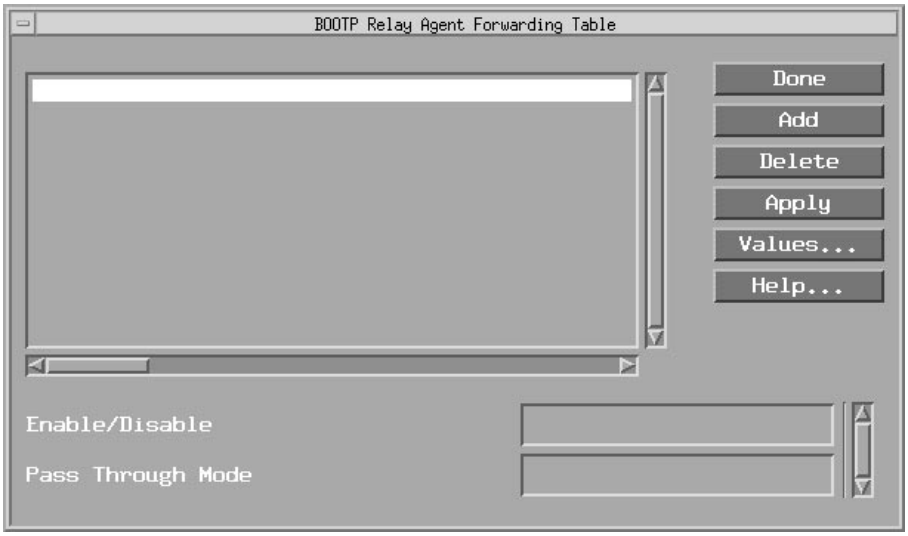

Figure 4-7. BOOTP Relay Agent Forwarding Table Window

3. **Click on Add.**

   The BOOTP Addresses window appears (Figure 4-8).

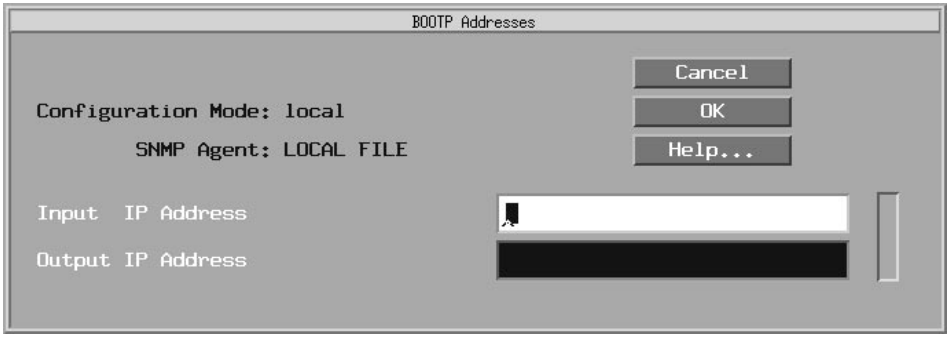

Figure 4-8. BOOTP Addresses Window

4. **Specify the input IP address and output IP address.**

   For help, refer to the parameter descriptions that follow this procedure.

5. **Click on OK.**

The BOOTP Relay Agent Forwarding Table window lists the connector and input IP address on the left, and the connector and output IP address on the right.

If you enter an IP address of an interface that is not configured, `???` appears instead of the connector (for example, `??? 192.32.23.3`). If you configure the IP address, Site Manager replaces the `???` with the appropriate connector.

6. **Click on Done to exit the window.**

BOOTP Relay Agent Interface Parameters

Parameter:	**Input IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP interface that receives BOOTP request packets from an external network. This interface must have BOOTP configured on it.
Instructions:	Enter the IP address of the interface through which the router will receive BOOTP requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.3

Parameter:	**Output IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP interface that forwards BOOTP request packets to an external network.
Instructions:	Enter the IP address of the interface through which the router will forward BOOTP requests.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.3.2.1.4

Creating the BOOTP Client Interface Table

The *upstream router* is a booting router's next-hop router. By default, the booting router's synchronous interfaces automatically try to get IP addresses from the upstream router. This is the EZ-Install process.

If the AN/ANH/ARN using EZ-Install gets its address from the upstream router, and the upstream router's interface to the AN/ANH/ARN is a Frame Relay group access PVC, you must use Site Manager to connect to the upstream router and create a BOOTP client interface table (in addition to a BOOTP relay agent forwarding table).

Note: You do not need to create a BOOTP client interface table if the Frame Relay PVC is configured to operate in direct access mode, or if the circuit is configured to operate with the Bay Networks Standard (HDLC encapsulation) protocol.

The BOOTP client interface table allows you to specify and pair the IP address of the AN/ANH/ARN with the DLCI of the Frame Relay group access PVC.

Note: If you are using EZ-Install over Frame Relay, you can have up to 20 PVCs for a single Frame Relay interface on the upstream router. If you have more than 20 PVCs on the interface where EZ-Install is occurring, the EZ Install process may fail. To ensure that the process does not fail, configure no more than 20 PVCs for a Frame Relay interface.

For more information about the DLCI and Frame Relay, refer to *Configuring Frame Relay Services*.

To create the BOOTP client interface table, begin at the BOOTP Relay Agent Interface Table window (refer to Figure 4-6) and proceed as follows:

1. **Click on Client I/F.**

   The BOOTP Client Interface Table window appears (Figure 4-9).

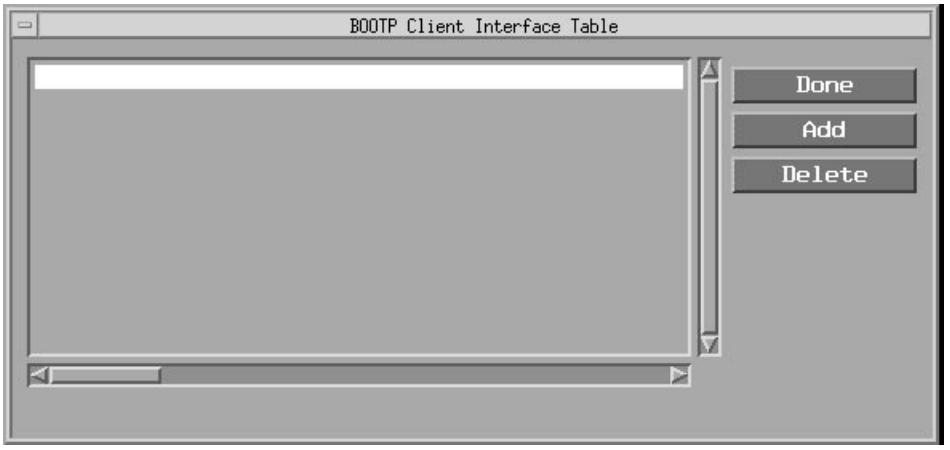

Figure 4-9. BOOTP Client Interface Table Window

2. **Click on Add.**

   The BOOTP Client Interface Address window appears (Figure 4-10).

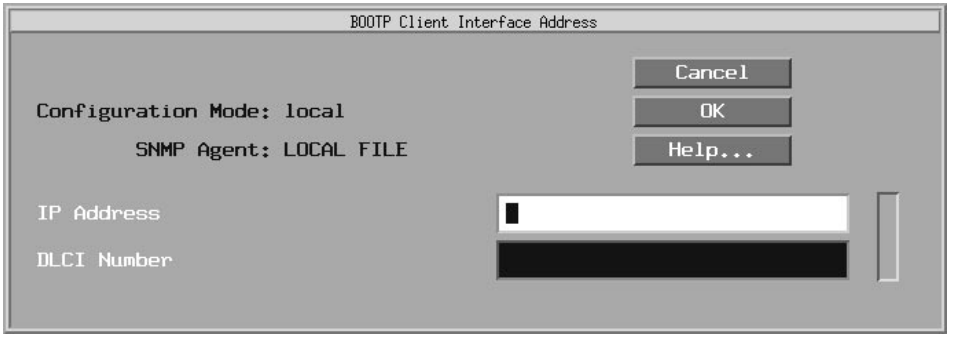

Figure 4-10. BOOTP Client Interface Address Window

3. **Enter the AN/ANH/ARN IP address and its associated DLCI number.**

   For help, refer to the parameter descriptions that follow this procedure.

4. **Click on OK.**

The BOOTP Client Interface Table window now lists the client IP interface and the DLCI number you added.

5. **Click on Done to exit the window.**

BOOTP Client Interface Parameters

Parameter:	**IP Address**
Default:	None
Options:	Any valid IP address
Function:	Specifies the IP address of the AN/ANH/ARN that is using EZ-Install. This parameter applies only to a Frame Relay group access PVC connection.
Instructions:	Enter the IP address (in dotted decimal notation) of the AN/ANH/ARN interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.3

Parameter:	**DLCI Number**
Default:	None
Range:	16 to 1007
Function:	Specifies the identification number of the upstream router's PVC to the AN/ANH/ARN. The Frame Relay network uses the DLCI number to direct data flow from the AN/ANH/ARN to the upstream router.
Instructions:	Enter the number in decimal format. Use the DLCI number assigned by your Frame Relay service provider.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.8.1.1.1.2

Chapter 5
Configuring the Router as a Network Boot Client

To enable an AN, ANH, or ARN for Netboot or Directed Netboot, you configure one or more router interfaces for network booting. You can do this using a Site Manager remote connection (as described in Chapter 4) or at the AN/ANH/ARN console using Technician Interface commands. This chapter describes how to use the

- **ifconfig** command to configure the AN/ANH/ARN's initial IP interface to the network
- **bconfig** command to specify the location and name of a software image and configuration file

To Configure This Boot Method	Complete These Sections
Netboot or Directed Netboot over a synchronous interface	• "Configuring the Router Boot Source" • "Configuring an IP Synchronous Interface for Network Booting"
Netboot or Directed Netboot over an Ethernet interface	• "Configuring the Router Boot Source" • "Configuring an Ethernet Interface for Network Booting"
Netboot or Directed Netboot of an ARN over a Token Ring interface	• "Configuring the Router Boot Source" • "Configuring a Token Ring Interface for Network Booting"

Working with a Person at the AN/ANH/ARN Site

Written for a person at the AN/ANH/ARN site, the guides *Installing and Operating BayStack ANH Systems* and *Installing and Operating BayStack ARN Routers* provide instructions for setting up the router for each of the boot options. These instructions assume that a network administrator provides the person at the AN/ANH/ARN site with the appropriate **ifconfig** and **bconfig** commands.

This chapter provides instructions for using the **ifconfig** and **bconfig** commands to configure Netboot and Directed Netboot. If you are not configuring the AN/ANH/ARN yourself, you can determine the appropriate syntax for these commands and provide the person at the router site with the exact command lines to use.

Configuring the Router Boot Source

To use Netboot, you use the **bconfig** command to specify that the AN/ANH/ARN configuration file or software image resides on the network. To use Directed Netboot, you use the **bconfig** command to specify the IP address of the server and the full pathname to the software image and configuration file.

bconfig Command Format

To configure an interface for Netboot, use the following format for the **bconfig** command:

bconfig -d [**image** | **config**]

To configure an interface for Directed Netboot, use the following format:

bconfig [**image** | **config**] [**local** | **network** [*<TFTP host> <TFTP pathname>*]]

You must use the **bconfig** command twice: once to specify the location of the software image, and again to specify the location of the configuration file.

Refer to Table 5-1 for a complete description of the **bconfig** command.

Table 5-1. bconfig Command Settings

Option	Description
image	Indicates the router's software image.
config	Indicates the router's configuration file.
local	Indicates that the specified file (image or config) resides in the router's local file system.
network	Indicates that the specified file (image or config) resides on a remote file system.
<TFTP host>	Specifies the IP address of the TFTP server. If both the software image and configuration file are on the network, both files must reside on the same host.
<TFTP pathname>	Specifies the complete pathname of the remote software image or configuration file.
-d	Reverts to the default values for the software image or configuration file and nullifies any previously specified IP address and pathname for the file, thus disabling Directed Netboot.

bconfig Command Examples

1. Configure the default Netboot procedure -- use a local image file and look for the configuration file over the network using BOOTP.

   bconfig -d image (or **bconfig image local**)
   bconfig -d config (or **bconfig config network**)

2. Use Netboot for both the boot image and configuration file.

   bconfig image network
   bconfig config network

3. Use a local configuration file and Directed Netboot for the boot image file.

   bconfig image network 21.3.5.62 /usr/mykernel.exe
   bconfig config local

4. Use a local boot image file and Directed Netboot for the configuration file.

   bconfig image local
   bconfig config network 21.3.5.62 /usr/anstartup/config

5. Use Directed Netboot for both the boot image and configuration file.

   bconfig image network 21.3.5.62 /usr/mykernel.exe
   bconfig config network 21.3.5.62 /usr/anstartup/config

Configuring the Netboot Interface

A router interface cannot communicate in an IP network without an IP address. Because an AN/ANH/ARN netboots over one of its synchronous, Ethernet, or Token Ring (ARN only) links, the Netboot interface must have a valid IP address.

You have two options for assigning an IP address to an interface:

- Use the Technician Interface **ifconfig** command to manually configure a synchronous, Ethernet, or Token Ring interface for Netboot or Directed Netboot.
- Configure the upstream router to support automated addressing for EZ-Install.

  Chapter 4 describes how to configure the upstream router to support EZ-Install by creating the BOOTP client interface table. “The Boot Process” section in Chapter 1 describes how the router automatically obtains an IP address during the EZ-Install process.

The following sections describe each use of the **ifconfig** command.

Configuring an IP Synchronous Interface for Network Booting

Configure a synchronous interface to the IP network using the following interface configuration command:

ifconfig [*synchronous options*] *<interface>* [*<IP address> <subnet mask>* [*<next hop address>*]]

The *synchronous options* variable indicates some combination of the following settings:

[**-d** | **-fr** [**-annexd** | **-lmi** | **-annexa**] | **-int_clk**]

Note: Insert a space to separate each command option from the next.

Table 5-2 describes the **ifconfig** command arguments for configuring an AN/ANH/ARN synchronous interface.

Table 5-2. ifconfig Command Settings for a Synchronous Interface

Setting	Description
Default Setting	
-d	Resets the router's IP interface settings to the default values. This setting tries four WAN configurations in the following order until it finds the correct type for the router's connection to the network: 1. Bay Networks HDLC encapsulation (also referred to as Bay Networks Standard Point-to-Point) with external clocking 2. Frame Relay Annex D 3. Frame Relay LMI 4. Frame Relay Annex A
Frame Relay Settings	
-fr	Configures the router's synchronous port as a Frame Relay connection. With this setting, use one of the following options to specify a DLCMI setting: **-annexd**, **-annexa**, or **-lmi**.
-annexd **-annexa** **-lmi**	When one of these options is used with the **-fr** setting, it specifies a DLCMI setting. Use the same setting as the network to which the router's Frame Relay interface is connected. The default setting for Frame Relay is **-annexd**.
Internal Clocking Setting	
-int_clk	Sets the synchronous port to internal clocking at 1.25 MB/s. If you do not specify this setting, the router defaults to external clocking.
IP Connector Setting	
<interface>	Specifies the IP connector you are configuring. Use the format **com**<*port no.*>.
IP Address Settings	
<IP address>	Specifies the IP address of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<subnet mask>	Specifies the IP subnet mask of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<next hop address>	Specifies the IP address of the next-hop router. Provide this address in dotted decimal notation. Specify this address only if there are intermediate routers between the router and the BOOTP server.

Configuring an Ethernet Interface for Network Booting

To configure an AN/ANH/ARN Ethernet interface for network booting, use the following command format:

ifconfig [**-d**] *<interface>* [*<IP address>* *<subnet mask>* [*<next hop address>*]]

Table 5-3 describes the **ifconfig** command arguments for configuring the router's Ethernet interface.

Table 5-3. ifconfig Command Settings for an Ethernet Interface

Setting	Description
Default Setting	
-d	Resets the router's IP interface settings to the default values. Resetting an Ethernet interface makes it inactive in the network booting process. (The output of the **getcfg** command shows the default as None.)
IP Connector Setting	
<interface>	Specifies the IP connector you are configuring. Use the format **xcvr**<*port no.*>.
IP Address Settings	
<IP address>	Specifies the IP address of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<subnet mask>	Specifies the IP subnet mask of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<next hop address>	Specifies the IP address of the next-hop router. Provide this address in dotted decimal notation. Specify this address only if there are intermediate routers between the router and the BOOTP server.

Configuring a Token Ring Interface for Network Booting

To configure an ARN Token Ring interface for network booting, use the following command format:

ifconfig [**-d**] [**-r**<*speed*>] *<interface>* [*<IP address>* *<subnet mask>* [*<next hop address>*]]

Table 5-4 describes the **ifconfig** command arguments for configuring the router's Token Ring interface.

Table 5-4. ifconfig Command Settings for a Token Ring Interface

Setting	Description
Default Setting	
-d	Resets the router's IP interface settings to the default values. Resetting a Token Ring interface makes it inactive in the network booting process. (The output of the **getcfg** command shows the default as None.)
IP Connector Setting	
-r<*speed*>	Specifies the speed of the Token Ring interface. Enter either **16** or **4** (Mb/s). The default is 16 Mb/s.
<interface>	Specifies the IP connector you are configuring. Use the format mau<*port no.*>.
IP Address Settings	
<IP address>	Specifies the IP address of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<subnet mask>	Specifies the IP subnet mask of the interface you set with *<interface>*. Provide this address in dotted decimal notation.
<next hop address>	Specifies the IP address of the next-hop router. Provide this address in dotted decimal notation. Specify this address only if there are intermediate routers between the router and the BOOTP server.

Enabling and Disabling Interfaces with ifconfig

To enable or disable an AN/ANH/ARN interface for the network boot process, use the following command formats:

ifconfig -disable *<interface>*
ifconfig -enable *<interface>*

Table 5-5 describes the **ifconfig** command arguments for enabling and disabling interfaces for network booting.

Table 5-5. ifconfig Settings to Enable and Disable Netboot Interfaces

Setting	Description
<interface>	Specifies the IP connector you are enabling or disabling for network booting. Use one of the following formats: **xcvr***<port no.>* **com***<port no.>* **mau***<port no.>*

ifconfig Command Examples

1. Configure the current interface for the default Netboot procedure.

   ifconfig -d

2. Specify the IP address and subnet mask of the first Ethernet Netboot interface.

   ifconfig xcvr1 21.3.5.62 255.255.255.0

3. Specify the IP address and subnet mask of the second Ethernet Netboot interface.

   ifconfig xcvr2 21.3.5.61 255.255.255.0

4. Configure the IP address and Frame Relay DLCMI of the third synchronous Netboot interface.

   ifconfig com3 21.3.5.62 -fr -annexa

5. Specify the IP address and subnet mask of the first Token Ring interface on an ARN.

   ifconfig mau1 21.3.4.77 255.255.255.0

Verifying Your Configuration

You can use the **getcfg** command to verify

- Whether the router is set to boot using a local or remote software image
- Whether the router is set to configure using a local or remote configuration file
- The configuration of the synchronous, Ethernet, and Token Ring (ARN only) connectors

Enter the following Technician Interface command to display the AN/ANH/ARN startup options:

getcfg

The following sample response shows the default settings for an AN or ANH with one Ethernet and two synchronous interfaces:

```
Boot Options

   boot image=local
   boot config=network

Netboot Parameters:

   XCVR1..None
   COM1...EZ-Install
   COM2...EZ-Install
```

The following sample response shows the settings for an ARN with one Ethernet, one Token Ring, and five synchronous interfaces:

```
Boot Options

   boot image=local
   boot config=network

Netboot Parameters:

   MAU1...None
   XCVR2..None
   COM1...EZ-Install
   COM2...EZ-Install
   COM3...EZ-Install
   COM4...EZ-Install
   COM5...EZ-Install
```

What to Do Next

You can now boot the router over the network, assuming that you already

- Configured a UNIX workstation to support network booting, as described in Chapter 3
- Prepared configuration and boot image files and placed them in the appropriate locations for your boot configuration, as described in Chapter 4

Whenever you boot the router, it should start routing traffic according to the configuration file it obtains from the BOOTP server.

You use the Site Manager Statistics Manager to view traffic statistics and the Event Log to determine whether the AN/ANH/ARN is routing traffic. Refer to *Managing Routers and BNX Platforms* for instructions on using the Statistics Manager and Events Manager tools.

If the AN/ANH/ARN does not begin routing traffic after booting, refer to Appendix A of this guide.

Chapter 6
Managing ANH Repeater Ports

You manage ANH repeater ports using Site Manager software. This chapter describes

- Enabling and Disabling ANH Repeater Ports
- Testing and Resetting ANH Repeater Ports

Enabling and Disabling ANH Repeater Ports

Use the following procedure to enable or disable the repeater ports on an ANH.

1. **From the Site Manager window, which appears at Site Manager startup, select Tools > Configuration Manager > Dynamic.**

   The Configuration Manager window appears, displaying the realtime router hardware and software configuration.

2. **From the Configuration Manager window, select Platform > Setup Repeater > Port Status.**

   The Port Status window appears, allowing you to enable or disable the ports on the router.

   Figure 6-1 shows the port status window for the 8-port ANH. Figure 6-2 shows the port status window for the 12-port ANH.

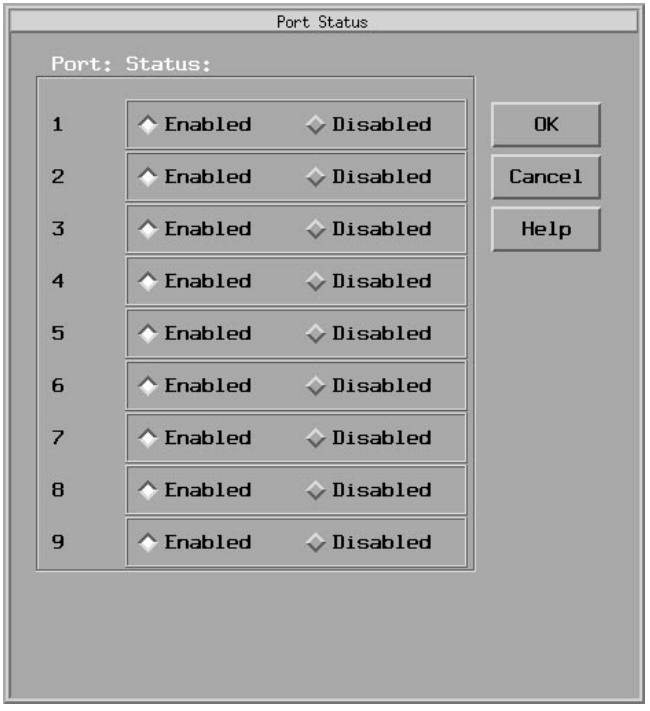

Figure 6-1. 8-Port ANH Port Status Window

Note: The ninth port is the AUI interface from the 8-port ANH router to the repeater. To disable the connection, disable the Ethernet circuit on Port 9.

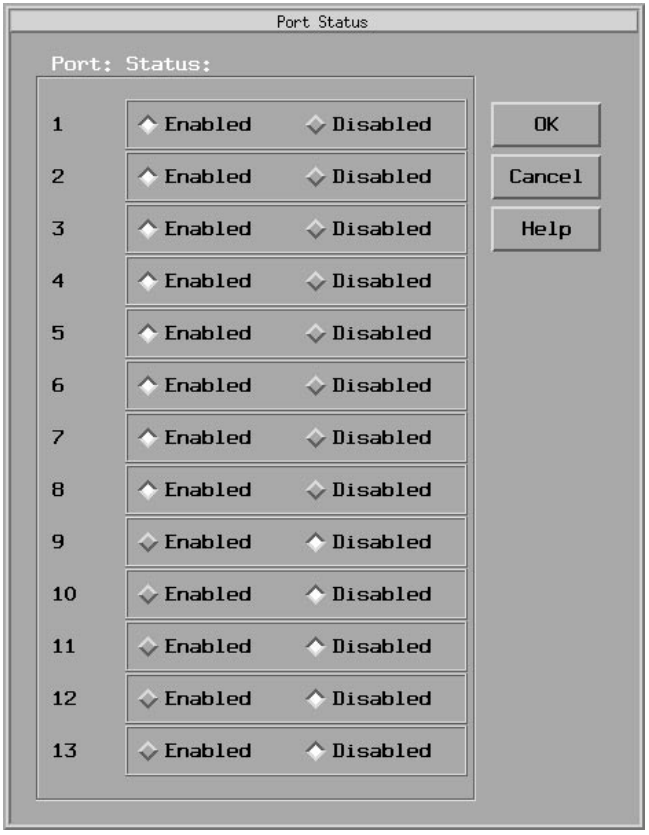

Figure 6-2. 12-Port ANH Port Status Window

Note: The thirteenth port is the Ethernet connection from the router base board to the repeater module. You disable the repeater by disabling Port 13.

3. **To change the status of a port, click on Enabled or Disabled to the right of the port number.**
4. **When you are finished, click on OK to exit the window and save your changes.**

Testing and Resetting ANH Repeater Ports

Use the following procedure to reset and test ANH repeater ports:

1. **From the Site Manager window, which appears at Site Manager startup, select Tools > Configuration Manager > Dynamic.**

   The Configuration Manager window appears, displaying the realtime router hardware and software configuration.

2. **From the Configuration Manager window, select Platform > Setup Repeater > Group Parameters.**

   The Group Parameters window appears (Figure 6-3), allowing you to reset the ANH or issue the self-test command.

Figure 6-3. Group Parameters Window

3. **Edit the parameters you want to change, using the parameter descriptions that follow as guidelines.**

4. **When you are finished, click on OK.**

   The Configuration Manager executes the action or actions you indicated in the Group Parameters window and closes the window.

Repeater Port Group Parameter Descriptions

Parameter:	**Reset**
Default:	NO_RESET
Options:	NO_RESET | RESET
Function:	Resets the repeater. The Configuration Manager tests each repeater port and records to a log file whether a port passed diagnostics. The reset does not affect the management counters defined in the RFC 1516 MIB, nor does it affect the status of the ports. However, it does disrupt traffic flow.
Instructions:	Accept the default, NO_RESET, or select RESET.
MIB Object ID:	1.3.6.1.2.1.22.1.1.4

Parameter:	**Selftest**
Default:	NO_SELFTEST
Options:	NO_SELFTEST | SELFTEST
Function:	Causes the router to perform an agent-specific test on itself. This test does not disrupt traffic flow.
Instructions:	Accept the default, NO_SELFTEST, or select SELFTEST.
MIB Object ID:	1.3.6.1.2.1.22.1.1.5

Chapter 7
Configuring a Data Collection Module

This chapter describes how to configure an optional Ethernet Data Collection Module (DCM) as an Ethernet remote monitoring (RMON) device, in the following sections:

- Ethernet DCM and RMON Overview
- Enabling a DCM Using Site Manager
- Managing the DCM Using Site Manager
- Managing the DCM Using the Technician Interface
- RMON Implementation Notes

Note: To run RMON on a Version 11.0 or higher Bay Networks router, the router must be running a version 1.4 or higher DCM image. If the router has an earlier version of DCM, the RMON Summary application returns an error message telling you that the router does not support RMON. For information on upgrading your router and the DCM image, refer to *Upgrading Routers from Version 7-10.xx to Version 11.0*. The upgrading manual also describes how to determine the version of DCM you are currently running.

Ethernet DCM and RMON Overview

The Ethernet DCM physically connects to AN/ANH/ARN base modules and to the ARN Ethernet expansion modules. It contains a Flash memory SIMM for its own boot image and configuration file. The DCM runs RMON agent software that

- Gathers statistics by monitoring packets on an Ethernet segment
- Stores the information according to the RMON MIB specification, in compliance with RFC 1757

To communicate with the RMON agent software on the DCM board, the router requires a software subsystem, called DCM *middleware* (DCMMW). This software subsystem enables and configures an installed DCM board.

Using Site Manager or the Technician Interface, you configure the DCMMW to

- Enable the DCM with a default configuration
- Modify the DCM configuration
- Boot the DCM
- Disable the DCM

To set up RMON configurations and to view statistics, use Optivity Design and Analysis software (AN and ANH only) or a third-party RMON network management application.

Remote Network Monitoring (RMON)

RFC 1757 is an extension of SNMP. It specifies a standard MIB that defines both parameters for recording statistics and the actual statistics themselves.

The purposes of RMON include

- Monitoring network performance.

  You can configure the DCM to continuously perform diagnostics and monitor network performance. If a network failure occurs, the DCM can store statistical information about the failure. The management stations can use this information to investigate the cause of the failure.

- Detecting and reporting problems.

  You can configure the DCM to recognize and continuously check for error conditions.

- Collecting information for problem solving.

  You can configure the DCM to give management stations information they need to solve problems. For instance, the DCM can identify the hosts on a network that generate the most traffic or errors.

Refer to “RMON Implementation Notes,” later in this chapter, for issues you should consider when using an Ethernet DCM for RMON.

The RMON Groups

The RMON agent runs on the DCM, and comprises a set of MIB groups. RFC 1757 defines the function and organization of these groups. Bay Networks implements the following groups in its RMON agent:

- Ethernet Statistics
- History Control
- Ethernet History
- Host
- HostTopN
- Matrix
- Filter
- Packet Capture
- Alarm
- Event

RMON groups contain *control* and *data tables*. Control tables contain *control parameters* that specify which statistics you want to access. You can view and change many entries in a control table. Data tables contain statistics that the agent obtains, and usually you can only view entries in these tables.

Some of the groups work together to provide a particular RMON function. For example, the History Control group and the Ethernet History group together provide the history capability in the RMON agent for the DCM.

The following sections indicate the function of each group and the tables that each group defines. Refer to RFC 1757 for the following information:

- A list of all the parameters that appear in a control table
- The read/write status of a control parameter
- The default values for control parameters with read/write status
- A list of all the objects that appear in a data table

Ethernet Statistics Group

The Ethernet Statistics group records data that the DCM measures on network interfaces. The DCM creates one entry for the Ethernet interface that it monitors on a device and places the entry in the EtherStatsTable. The EtherStatsTable also contains control parameters for this group.

History Control Group and Ethernet History Group

The History Control and Ethernet History groups work together to control and record the periodic statistical sampling of data from various types of networks. The historyControlTable and etherHistoryTable comprise the two groups.

Host Group

The Host group identifies hosts on the network by recording the source and destination MAC addresses in good packets, and places the information in the hostTable. This group also records the time it discovered a host on the network in the hostTimeTable. The hostControlTable specifies control parameters and contains information about the monitoring process.

HostTopN Group

The HostTopN group ranks hosts according to a statistic type. For example, you might want to rank the hosts by the number of errors they generate. Control parameters for this group appear in the hostTopNControlTable, and data that this group generates appears in the hostTopNTable. To use the HostTopN group, you must set up the Host group.

Matrix Group

The Matrix group stores statistics for an interchange between interfaces at different addresses. This group's control parameters, such as the interface that starts the interchange, appear in the matrixControlTable. When the Matrix group receives information from a good packet, it places data in both the matrixSDTable and the matrixDSTable.

Filter Group

The Filter group specifies what type of packets the DCM should capture. Filter control parameters, such as the minimum length of the packets to capture, appear in the filterTable. Associated with each filter is a *channel* (a specific path along which data flows). Control parameters in the channelTable define how and where the filtered packets flow.

Packet Capture Group

The Packet Capture group enables the capture of packets that satisfy the Filter group control parameters. For example, you can specify the maximum number of octets from each packet that the group should store in the captureBufferTable. To use the Packet Capture group, you must set up the Filter group.

Alarm Group

The Alarm group takes statistical samples from variables in the DCM and compares them to previously configured thresholds. If the monitored variable crosses a threshold, the DCM generates an event. The DCM will not generate another event for that threshold until the opposite threshold is crossed. Alarm control parameters, such as variable definitions, polling period, and threshold parameters, appear in the alarmTable. To use this group, you must set up the Event group.

Event Group

The Event group controls the generation and notification of events from the router. This group consists of the eventTable and the logTable. Each entry in the eventTable describes the parameters of the event that can be generated. For each event entry, there is an associated condition elsewhere in the MIB that can generate the event. The MIB may also contain an associated function that is executed when the event is generated. Each eventEntry may optionally specify that

- A log entry be created whenever the event occurs.
- Notification should occur by way of SNMP trap messages. In this case, the associated eventCommunity object gives the community for the trap message.

For More Information about RMON

The following documents provide more detail:

- RMON MIB (RFC 1757)
- The user guide for Optivity Design and Analysis network management software

Enabling a DCM Using Site Manager

To enable a newly installed Ethernet DCM option by creating the DCM software subsystem (DCMMW):

1. **From the Configuration Manager window, select Platform > DCM 11.0 and later > Create Base Module DCM.**

Note: On ARN models only, you can enable a DCM on both an Ethernet base module and an Ethernet expansion module. To create the DCM software subsystem on an ARN expansion module with an installed DCM, select **Platform > DCM 11.0 and later > Create Expansion Module DCM**.

The Edit Base Module DCM Parameters window appears (Figure 7-1).

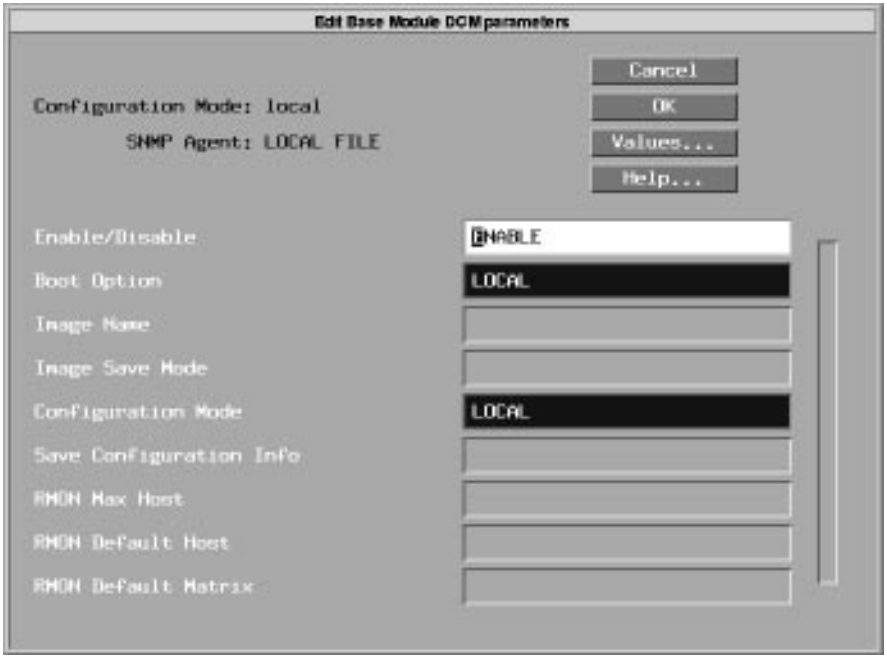

Figure 7-1. Edit Base Module DCM Parameters Window

Note: If you chose the **Create Expansion Module DCM** option for an ARN, the Edit Expansion Module DCM Parameters window appears, with parameters identical to those in the Edit Base Module DCM Parameters.

2. **To accept the default configuration, click on OK. Or to customize the configuration, continue with Step 3.**
3. **Edit the parameters you want to change.**

   Use the descriptions that follow as guidelines.
4. **When you are finished, click on OK.**

Caution: Configuration changes are effective only after you reboot the DCM board. To do this, use the Edit Base Module DCM Parameters window (or the Edit Expansion Module DCM Parameters window) to disable and then reenable DCM.

DCM Global Parameter Descriptions

Parameter:	**Enable/Disable**
Default:	ENABLE
Options:	ENABLE | DISABLE
Function:	Enables or disables DCMMW (the DCM software subsystem), and therefore the DCM board.
Instructions:	To enable the DCM board, select ENABLE. To disable the DCM board, select DISABLE. Use this parameter to reboot the DCM board by enabling, then disabling DCMMW.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.3

Parameter:	**Boot Option**
Default:	LOCAL
Options:	LOCAL | DOWNLOAD
Function:	Specifies whether the DCM board uses the image in its own Flash memory for booting, or an image copied from the router's file system to DCM shared memory (DRAM).
Instructions:	Select LOCAL to specify the image file in DCM local Flash memory as the DCM boot image. Select DOWNLOAD to specify an image file on the router's Flash memory as the DCM boot image. When the DCM board boots in DOWNLOAD mode, DCMMW software moves a copy of the image to DCM shared memory. You specify the downloaded image with the Image Name parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.8

Parameter:	**Image Name**
Default:	None, but you must specify an image name when the Boot Option parameter is set to DOWNLOAD.
Options:	An ASCII text string, no more than 255 characters
Function:	Specifies the pathname of a DCM boot image in the router's file system. The image name must be a fully qualified filename, including both volume and filename.
Instructions:	Enter the volume and filename for the image you want the DCM board to boot, using the form <*volume_number:filename*>; for example, **1:dcm_image**.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.7

Parameter:	**Image Save Mode**
Default:	SAVE
Options:	SAVE | NO SAVE
Function:	Specifies whether the DCM saves the active image into its local Flash memory or keeps the image in shared DRAM only.
Instructions:	To save the DCM boot image file to the DCM board's local Flash memory (writing over the existing saved image), select SAVE. Select the NO SAVE option if you do not want to save the DCM boot image file (the image remains in DRAM until the next time the DCM board boots).
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.9

Parameter:	**Configuration Mode**
Default:	LOCAL
Options:	LOCAL | SHARED MEMORY
Function:	Specifies whether to use configuration information in the DCM board Flash memory or in the DCM board's shared memory space (DRAM).
Instructions:	Select LOCAL to use the default configuration information in the DCM local Flash memory. Select SHARED MEMORY to use the configuration information in the DCM DRAM, written by DCMMW from the router's file system.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.10

Parameter:	**Save Configuration Info**
Default:	WRITE
Options:	WRITE | NO WRITE
Function:	Specifies whether to write the configuration information in DRAM to the DCM board's Flash memory.
Instructions:	Select WRITE to save the configuration information in DRAM to the DCM board's Flash memory (writing over the existing configuration file). Select NO WRITE to avoid overwriting the DCM board's configuration file.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.11

Parameter:	**RMON Max Host**
Default:	500
Range:	100 to 8128
Function:	Relates to the RMON Host group. Indicates the maximum number of host addresses to be collected in each entry of the RMON host control table. The maximum limit depends on the amount of Flash memory available in the DCM. When the host control table reaches the maximum value, the DCM deletes entries based on an LRU (least recent used) algorithm.
Instructions:	Recommended values, based on DCM memory configurations, are 2 to 4 MB: 2048 8 MB: 4096 16 MB: 8128 To verify the number of hosts configured, check the MIB object wfDCMmwRMONHost using the Site Manager Statistics tool.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.12

Parameter:	**RMON Default Host**
Default:	Disable
Options:	Enable | Disable
Function:	Specifies whether to create the RMON Host Control Table at every boot. Some RMON network management applications expect the DCM to set up a host configuration. Others enable and disable their own configurations during normal operations. Note that the DCM allows only one instance of the host control table.
Instructions:	Select Enable to create the RMON Host Control Table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON host control table at boot time.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.13

Parameter:	**RMON Default Matrix**
Default:	Disable
Options:	Enable | Disable
Function:	Relates to the RMON Matrix group. Specifies whether or not to create the RMON Matrix Control Table at every boot. Some RMON network management applications expect the DCM to set up a matrix configuration. Others enable and disable their own configurations during normal operations. Note that the DCM allows only one instance of the matrix control table.
Instructions:	Select Enable to create the RMON Matrix Control Table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON Matrix Control Table at boot time.
MIB Object ID:	1.3.6.1.4.1.18.3.3.2.16.2.1.14

Managing the DCM Using Site Manager

To manage the installed DCM, you can use Site Manager to

- Change the DCMMW configuration.
- Enable or disable a default RMON Max Host, Default Host, and Default Matrix configuration.
- Activate, temporarily disable, and boot the DCM board.
- Deactivate the DCM by disabling the DCMMW software subsystem.

You use Optivity Design and Analysis software or a third-party RMON network management application to set up RMON configurations and to view statistics.

Activating the DCM

To activate the DCM:

1. **From the Configuration Manager window, select Platform > DCM 11.0 and later > Global > Base Module DCM.**

   The Edit Base Module DCM Parameters window appears (refer to Figure 7-1).

Note: On ARN models, you can also activate the DCM on an Ethernet expansion module. To do this, select **Platform > DCM 11.0 and later > Global > Expansion Module DCM**. The Edit Expansion Module DCM Parameters window appears. The parameters in this window are identical to those in the Edit Base Module DCM Parameters window.

2. **Set the Enable/Disable parameter to ENABLE.**
3. **Click on OK to exit the window.**

Disabling the DCM

To temporarily disable an installed DCM:

1. **From the Configuration Manager window, select Platform > DCM 11.0 and later > Global > Base Module DCM.**

   The Edit Base Module DCM Parameters window appears (refer to Figure 7-1).

Note: On ARN models, you can also disable the DCM on an Ethernet expansion module. To do this, select **Platform > DCM 11.0 and later > Global > Expansion Module DCM**. The Edit Expansion Module DCM Parameters window appears. The parameters in this window are identical to those in the Edit Base Module DCM Parameters window.

2. **Set the Enable/Disable parameter to DISABLE.**
3. **Click on OK to exit the window.**

If disabling the board does not work, you can delete the software subsystem to totally shut down the DCM.

Booting the DCM

To reboot an installed DCM board, disable and then reenable the DCM as described in the previous sections.

Changing the DCM Configuration Parameters

To edit the DCMMW configuration parameters for an installed DCM board:

1. **From the Configuration Manager window, select Platform > DCM 11.0 and later > Global > Base Module DCM.**

   The Edit Base Module DCM Parameters window appears (Figure 7-2).

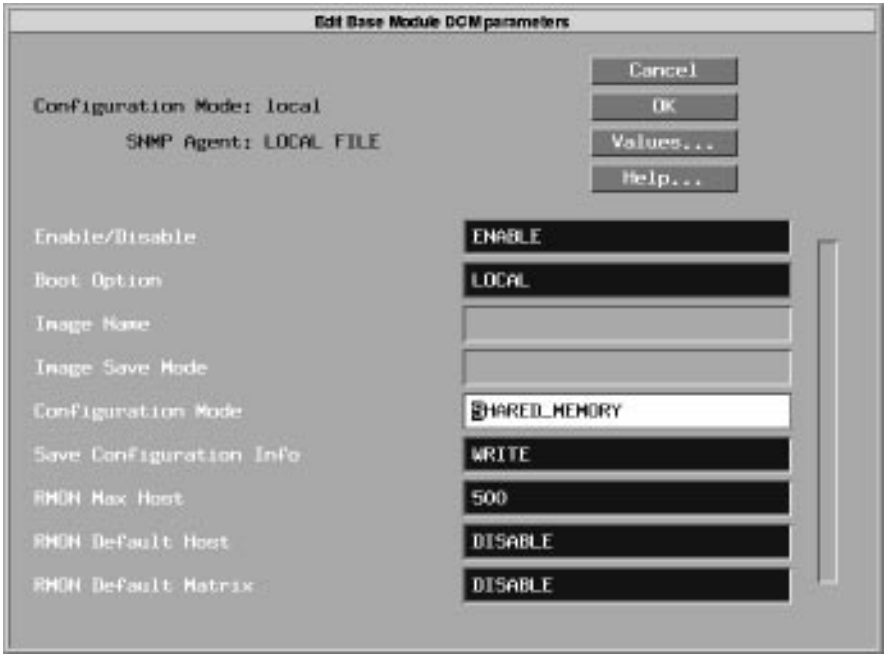

Figure 7-2. Edit Base Module DCM Parameters Window

Note: On ARN models, you can also change the DCM configuration parameters on expansion modules that support the DCM. To do this, select **Platform > DCM 11.0 and later > Global > Expansion Module DCM**. The Edit Expansion Module DCM Parameters window appears. The parameters in this window are identical to those in Edit Base Module DCM Parameters.

2. **Set the Enable/Disable parameter to DISABLE.**
3. **Click on OK.**
4. **Select Platform > DCM 11.0 and later > Global > Base Module DCM again to return to the Edit Base Module DCM Parameters window.**
5. **Set the Configuration Mode parameter to SHARED MEMORY.**
6. **To use this configuration in subsequent boots, set the Save Configuration Info parameter to WRITE.**
7. **Set the remaining configuration parameters (RMON Max Host, RMON Default Host, and RMON Default Matrix) to the desired values.**

   For information, see "DCM Global Parameter Descriptions," earlier in this chapter.
8. **Set the Enable/Disable parameter to ENABLE.**
9. **Click on OK.**

Deleting the DCM Software Subsystem

The router requires the DCMMW software to communicate with the DCM board. Deleting DCMMW deactivates the DCM board.

Note: Always try **disabling** the DCM board by setting the Enable/Disable parameter to Disable before you delete the DCMMW software.

To completely deactivate the DCM board:

1. **From the Configuration Manager window, select Platform > DCM 11.0 and later > Delete DCM, and then select one of the following:**
   - **Base Module DCM only** - to remove the DCM software subsystem from an AN or ANH, or from an ARN base module.
   - **Expansion Module DCM only** - to remove the DCM software subsystem from an ARN Ethernet expansion module.
   - **All DCMs** - to remove the DCM software subsystem from all modules on the current platform.

   The Configuration Manager displays a confirmation prompt.

2. **Click on OK.**

   The Configuration Manager deletes the DCM software subsystem on the modules you selected. The deletion brings the DCM board (or boards) completely down.

After deleting the DCM configuration, you reactivate the DCM board by selecting **Platform > DCM 11.0 and later > Create Base Module DCM** (or on ARN models you can choose Create Expansion Module DCM) to re-create the DCMMW record.

Managing the DCM Using the Technician Interface

You can use Technician Interface commands to

- Enable, disable, and reboot the DCM board (**enable/disable dcm** scripts).
- Download a new DCM software image (**dcmload** script).
- Display (**show** command) or modify (**set/get** commands) DCMMW configuration parameters.

Caution: Avoid running scripts that continually issue Technician Interface commands while you are running another RMON network management application. This combination can cause the SNMP agent to fill the system buffers with RMON data, leading to a system restart.

For more information about using the Technician Interface to access the DCM MIB objects, refer to *Using Technician Interface Software* and *Using Technician Interface Scripts*.

Changing DCM Configuration Parameters

Modifying DCM or RMON parameters by issuing **set** and **commit** commands with the MIB object ID is equivalent to modifying parameters using Site Manager.

For example, issue the following commands to change the maximum host configuration on the base module:

```
set wfDCMmw.wfDCMmwRMONMaxHost.0 1200;commit
disable dcmmw base
enable dcmmw base
```

Or, to change the maximum Host configuration on an ARN expansion module, issue the following command:

set wfDCMEntry.wfDCMmwRMONMaxHost.2 1200;commit
disable dcm expansion
enable dcm expansion

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Consider the following when changing DCM configuration parameters:

- Set the value of wfDCMmw.wfDCMmwCfgMode.0 to DCMMW_CFG_LOAD_SHMEM before changing other object values.
- After changing any DCM object values, reboot by disabling, then enabling the DCM to initialize the changes.
- To use a configuration change after rebooting the DCM, set the wfDCMmwWriteConfigInfo parameter to DCMMW_CFG_WRITE so the DCM saves the new information to its Flash memory.

RMON Implementation Notes

Read the following sections to learn about RMON memory use and interoperability issues that you should consider when using RMON network management applications with the DCM.

- RMON Applications
- RMON Memory Use
- Interoperability Issues and Memory Use for RMON Groups

These sections assume that you have a good understanding of each RMON group, and do not refer to the low-level details of the MIB, such as RMON MIB objects. Refer to "Remote Network Monitoring (RMON)," earlier in this chapter, and RFC 1757 for information about each RMON group.

RMON Applications

Some network management applications automatically set up their own configurations for an RMON group, without checking to see if the RMON agent already has a default configuration. In addition, when you terminate those applications, they may not remove the configurations they set up for the RMON agent. These features can result in the RMON agent using excessive amounts of memory and processing power.

Example

When you enable a DCM, the RMON agent automatically creates a History configuration. Suppose you then start a third-party RMON History application, which creates its own History configuration for the agent. The RMON agent stores the data in two places, wasting memory.

In addition, when you terminate the third-party RMON application, it does not remove its History configuration, using memory and processing power indefinitely.

You can release these resources only by using another application, such as the SNMP tool or network management station, or by resetting the DCM. If you use too many resources for an RMON task, the DCM can run out of memory for other RMON tasks and performs more slowly.

RMON Memory Use

The total amount of RMON memory depends on the DRAM in the DCM (Table 7-1).

Table 7-1. DRAM and RMON Memory Size

Installed DRAM (MB)	RMON Memory in Bytes
2	162,578
4	2,077,330
8	5,222,034
16	12,561,042

NOTE: If the RMON memory pool is full or if the RMON agent reaches an implementation limit, the agent responds to an SNMP **set** command on an RMON control table entry with an SNMP GEN-ERROR.

The following sections describe how much memory you need to

- Configure an RMON group (for example, to configure the Matrix group or to configure Filter and Packet Capture groups).
- Store the data for an RMON group (for example, to store the packets a DCM captures).

In the following sections, the word *configuration* means the set of control tables for a group. For example, a Matrix configuration includes only the matrixControlTable. Note that you can create more than one configuration for some RMON groups. For example, you can create more than one History configuration, allowing you to specify different intervals for sampling statistics.

Interoperability Issues and Memory Use for RMON Groups

You should understand the following issues about each RMON group's memory requirements and ability to operate with third-party RMON network management applications.

Statistics Group

When you enable the DCM, the RMON agent automatically creates a Statistics configuration that records data for each network interface. Through your RMON network management application, you can create as many Statistics configurations as memory permits, up to the RMON limit of 65,535 configurations.

If you create multiple configurations, it is possible to collect the same set of statistics for the same interface in multiple data tables. The absolute values of those statistics may vary from table to table, because the baseline of each statistics counter occurs when you create a configuration. You may prefer, however, to use only one Statistics configuration to conserve memory for other RMON groups.

You need 200 bytes of memory for each Statistics configuration.

History Group

When you enable the DCM, the RMON agent automatically creates a History configuration that collects History data at two intervals. The first configuration provides short-term history by sampling statistics every 30 seconds and holding up to 50 samples (in RMON terms “buckets”). The second configuration provides long-term history by sampling statistics every 30 minutes and holding up to 50 buckets.

Through your RMON network management application, you can create as many History configurations as memory permits, up to the RMON limit of 65,535 configurations.You can also set the number of buckets that a particular History configuration uses to as many as available memory allows. If you request more buckets than memory allows, the agent allocates enough buckets to fill available memory.

You need 504 bytes of memory for each History configuration (252 bytes each for the short-term and long-term History configurations).

The History data requires 52 bytes of memory per bucket. You calculate the total memory (in bytes) that you need to store the data as follows:

Number of buckets * 52 * 2 History configurations

This calculation shows that you need approximately 5.1 KB for the default setting of 50 buckets.

Host Group

When you enable the DCM, the default setting (Disable) for the RMON Default Host parameter does not create a Host configuration. To create a Host configuration, set the RMON Default Host parameter to Enable before you enable the DCM as described earlier in the "Activating the DCM" section.

Some RMON network management applications expect the DCM to set up a Host configuration, while others set up their own configurations.

Note: The RMON agent allows you to create only one Host configuration. Be sure to set the RMON Default Host parameter according to the expectations of the RMON network management application.

The Host configuration requires 148 bytes. The Host data requires 105 bytes of memory per host address that the DCM detects on a segment.

You specify the maximum number of host addresses that appear in the Host configuration by setting the RMON Max Host parameter when you enable a DCM. If there is not enough memory for the number of hosts you request, the RMON agent sets the RMON Max Host parameter to the highest possible value. Depending on the DCM memory configuration, the number of addresses can range from 100 to 8,128. Table 7-2 shows recommended values for this parameter.

Table 7-2. Maximum Number of Hosts

Installed DRAM (MB)	Maximum Number of Hosts
2 to 4	2,048
5 to 8	4,096
9 to 16	8,128

You calculate the total memory (in bytes) that you need for the host data as follows:

105 * Value of the RMON Max Host parameter

HostTopN Group

To save memory and increase performance, there is no default configuration for the HostTopN group. You must create HostTopN configurations through your RMON network management application. You can create as many HostTopN configurations as memory permits, up to the RMON limit of 65,535 configurations.

Note: Before you create a HostTopN configuration, you must create a Host configuration.

Each HostTopN configuration requires 164 bytes. The HostTopN data requires 10 bytes of memory per host address that the DCM detects on a segment.

You calculate the total memory (in bytes) that you need for the HostTopN data as follows:

10 * Value for the RMON Max Host parameter

Refer to the previous section for information on setting the RMON Max Host parameter.

Matrix Group

When you enable the DCM, the default setting (Disable) for the RMON Default Matrix parameter prevents the DCM from setting up a Matrix configuration. To create a Matrix configuration, set the RMON Default Matrix parameter to Enable before you enable the DCM as described in the "Activating the DCM" section.

Some RMON network management applications expect the DCM to set up a Matrix configuration, while others set up their own configurations.

Note: The RMON agent allows you to create only one Matrix configuration. Be sure to set the RMON Default Matrix parameter according to the expectations of the RMON network management application.

The Matrix configuration requires 212 bytes. The Matrix data requires approximately 178 bytes of memory per source/destination pair that the DCM detects on a segment.

Filter and Capture Groups

Caution: The memory you need for a Filter/Capture configuration and for storing captured packets can easily exhaust all the available memory on a DCM, particularly if the filters are not selective.

You must create Filter and Capture configurations through your RMON network management application. You can create as many filters and capture buffers as memory permits, up to the RMON limit of 65,535 configurations.

Memory requirements vary greatly according to the size and number of the filters and the size of the capture buffer. In most cases, you need 3 to 5 KB of memory for the Filter and Packet Capture configuration.

The size of the capture buffer determines the amount of memory you need for the data. You can request the largest buffer size available by specifying a buffer size of -1 through your RMON network management application. When you specify -1 for the capture buffer size, the agent attempts to allocate a default buffer depending on the DRAM in the DCM (Table 7-3).

Table 7-3. Default Size for Capture Buffer

Installed DRAM (MB)	Default Buffer Size (KB)
2	32
4	64
8	256
16	512

You can also request a larger buffer size up to 15 MB. In any case, if there is not enough memory currently available to satisfy the request, the agent will provide a buffer that uses all available memory.

You can determine the maximum number of packets that an agent can capture in a buffer as follows:

buffer size/(packet slice size + 20 bytes)

Example

You specify a buffer size of 32 KB and a packet slice size of 1 KB. After checking the available memory, the RMON agent allocates the buffer size you requested. The buffer can hold a maximum of 32,768 / (1024 + 20) or 31 packets.

Note: The RMON agent allocates the full amount of memory you specify for the packet slice size to each packet, even if the packet size is smaller than this amount. For this reason, Bay Networks recommends that you set the packet slice size to the smallest size possible. The maximum packet size is 2 KB.

Alarm and Event Group

You configure the Alarm and Event group as a pair. The pair requires approximately 750 bytes of memory. In addition, for each occurrence of an event, the log uses about 150 bytes. You can store a maximum of 100 log entries for each event configuration.

Note: You can limit the size of event descriptions to reduce the memory requirements for event configurations.

The logTable is a read-only table. You can access this table using the specific eventIndex.

You can set alarms to RMON MIB variables only.

Appendix A
Troubleshooting Network Boot Problems

Use the information in the following sections of this appendix to resolve problems directly related to startup and connectivity with remote routers.

- Router Fails to Get IP Address
- Identifying Remote Connectivity Problems
- Resolving Connectivity Problems
- Maintaining the Router Software

Note: For most troubleshooting information, see *Troubleshooting Routers*.

Solving Startup Problems

This section helps you isolate and solve the four most common router startup problems. Refer to the appropriate section:

- Router Fails to Get IP Address
- Router Fails to Netboot
- Router Fails to Perform Directed Netboot
- Router Netboots, but Fails to Load Applications

Router Fails to Get IP Address

If a message at the router console indicates that the router failed to get an IP address from the upstream router, or if the upstream router is failing to receive BOOTP requests or respond to them, make sure that the network cable between the router's synchronous port and the upstream router is firmly connected. Then refer to the instructions in one of the following sections until you find and correct the problem:

- Upstream Router Not Receiving BOOTP Requests
- Upstream Router Not Sending BOOTP Responses

Contact the Bay Networks Technical Response Center if you follow the instructions in these sections and cannot find and correct the problem.

Upstream Router Not Receiving BOOTP Requests

If the upstream router is not receiving BOOTP request messages, use the **getcfg** command to display the router parameters and the **bconfig** and **ifconfig** commands to correct them if necessary. Refer to "Displaying Parameter Settings" and "Debugging the BOOTP Server" later in this appendix if you need instructions.

Upstream Router Not Sending BOOTP Responses

If the upstream router is receiving BOOTP request messages but failing to send BOOTP responses, use Site Manager to verify the following:

- The upstream router's interface to the AN/ANH/ARN is enabled.
- BOOTP is enabled on the circuit connecting the AN/ANH/ARN to the upstream router.
- The upstream router's link modules and drivers are loaded.
- The upstream router's IP protocol is enabled.
- The upstream router's BOOTP protocol is enabled.
- The BOOTP relay agent forwarding table associated with the upstream router shows a valid IP address that is configured on the IP router.
- The input IP address is correct.

- If you are using EZ-Install over a Frame Relay permanent virtual circuit (PVC) in group access mode, the upstream router's BOOTP client interface table is configured properly.

Router Fails to Netboot

If the router fails to receive the configuration file or image using a network boot option, first

- Make sure that all cables between the router and the BOOTP server are firmly connected.
- If using the **ifconfig** command, be sure to specify the boot image *krnl_an.exe* for an AN/ANH or *krnl_arn.exe* for an ARN.

Then refer to the instructions in the following sections until you find and correct the problem:

- Upstream Router Not Receiving BOOTP Requests
- Router Not Sending BOOTP Responses
- BOOTP Server Not Sending BOOTP Responses

If you have not isolated the problem to a specific interface, retrieve the number of BOOTP packets forwarded and dropped from all routers between the router and the BOOTP server. Refer to "Displaying the Number of Packets Forwarded and Dropped" later in this appendix.

Contact your local Bay Networks Technical Response Center if you perform the instructions in these sections and cannot find and correct the problem.

Upstream Router Not Receiving BOOTP Requests

If the upstream router is not receiving BOOTP request messages, do the following:

1. **Execute the Technician Interface getcfg command to display the router parameters and the bconfig or ifconfig command to correct them if necessary.**

   Refer to "Displaying Parameter Settings" and "Debugging the BOOTP Server" later in this appendix if you need instructions.

2. **Make sure that the AN/ANH/ARN's synchronous port configured for EZ-Install is cabled to the upstream router, or that the port configured for Netboot (synchronous, Ethernet, or Token Ring) is cabled properly.**

Router Not Sending BOOTP Responses

If a router (that is in the path from the AN/ANH/ARN to the BOOTP server) is receiving BOOTP request messages but failing to return BOOTP responses, do the following:

1. **Use Site Manager to make sure that the BOOTP relay agent forwarding table associated with the router shows an IP address that is configured on the IP router.**
2. **Make sure that the input IP address is correct. If the Hops count is lower than the router's position in the path, increase it.**

   Refer to "Creating the BOOTP Client Interface Table" in Chapter 4 if you need instructions.
3. **Use the Configuration Manager to make sure that BOOTP and IP are enabled on the incoming and outgoing interfaces.**
4. **Make sure that the link modules and drivers are enabled. Refer to** *Configuring Routers* **if you need instructions.**

BOOTP Server Not Sending BOOTP Responses

If the BOOTP server is receiving BOOTP requests but failing to respond to them, do the following:

1. **Follow the instructions in the section "Displaying the BOOTP Server's IP Routes" later in this appendix.**
2. **Follow the instructions in the section "Debugging the BOOTP Server" later in this appendix.**
3. **Make sure that the** */etc/inetd.conf* **file contains no more than one** `bootps` **entry.**

   If there is more than one entry, comment out the invalid entry. The valid entry should be

   ```
   bootps dgram udp wait root /etc/bootpd bootpd
   ```

4. **Make sure that the `tftp dgram` entry in the */etc/inetd.conf* file is correct for your system.**

   Refer to "Setting Up a TFTP Server" in Chapter 3.

5. **Refer to "Verifying the BOOTP Server Setup" later in this appendix.**

Router Fails to Perform Directed Netboot

If the AN/ANH/ARN fails to perform Directed Netboot, verify the following:

- The interface that connects the router to the TFTP file server is configured with an IP address.
- All necessary files are, in fact, residing on the TFTP file server.
- The boot file is *krnl_an.exe* for an AN/ANH or *krnl_arn.exe* for an ARN.

Contact your local Bay Networks Technical Response Center if you perform the instructions in these sections but still cannot find and correct the problem.

Router Netboots, but Fails to Load Applications

If the router Netboots a software image successfully, but displays an error message indicating that it cannot load specific applications, it is failing to retrieve files from the TFTP server that provided the software image. These files are necessary to perform functions such as running the protocols specified in the configuration file or displaying the log.

Do the following:

1. **Make sure that, after booting, you have at least one interface configured through which the file server that supplied the kernel image can be reached.**

   This is necessary for a router that has obtained its image over the network to load application or string files.

2. **Make sure that all the application and string files (files with *.exe* and *.str* filename extensions) reside in the same directory as the kernel image.**

3. **Verify that you have TFTP on the router. To determine this, display the router's `loadmap` screen message.**

   If *tftp.exe* is missing, load it onto the router.

4. **Use Site Manager to make sure that IP is enabled and TFTP is created in the AN/ANH/ARN configuration file.**

   Refer to "Verifying the BOOTP Server Setup" later in this appendix.

5. **Use Technician Interface commands to verify or correct the status of the synchronous, Ethernet, or Token Ring connectors used for network booting.**

   Refer to *Using Technician Interface Software* for instructions. Following are some examples of AN/ANH/ARN commands and their responses, as well as some connector and interface settings you should consider:

   - Enter the following command to display the router driver:

     get wfLinkModules.15.0

     On AN and ANH models, the response is

     ```
     wfLinkModules.wfANLoad.0 = 2147483648
     ```

     On ARNs, the response is

     ```
     wfLinkModules.wfARNLoad.0 = 2147483648
     ```

     The response indicates that the AN/ANH/ARN driver is configured to run in Slot 1 (the only AN/ANH/ARN slot).

     The decimal number `2147483648` represents Slot 1. If the setting is not `2147483648`, enter one of the following commands to correct it:

     set wfLinkModules.15.0 2147483648;commit (for AN/ANH models)
     set wfLinkModules.25.0 2147483648;commit (for ARNs)

To display the drivers that are configured to run, enter the following command:

get wfDrivers.*.0

A combination of the following settings should appear within the list of drivers, according to your AN/ANH/ARN configuration:

`wfDrivers.wfQsccSyncLoad.0 = 2147483648`	COM ports
`wfDrivers.wfQsccEnetLoad.0 = 2147483648`	Ethernet ports (nonrepeating)
`wfDrivers.wfRptrLoad.0 = 2147483648`	Ethernet repeater ports (ANH only)
`wfDrivers.wfTMS380Load.0 = 2147483648`	Token Ring ports

Use the **set** command to correct any settings that are incorrect. For example, if the router has a Token Ring port and the `wfDrivers.wfTMS380Load.0` setting is not `2147483648`, enter the following command to correct it:

set wfDrivers.wfTMS380Load.0 2147483648;commit

- If the router is Netbooting with a synchronous connector, enter the following command to display the information about the connector, where <*connector*> is the connector number:

  get wfSyncEntry.*.1.<*connector*>

  Make sure that external clocking is set.

- If the router is Netbooting with an Ethernet connector, enter the following command to display the information about the connector, where <*connector*> is the connector number:

  get wfCSMACDEntry.*.1.<*connector*>

- If the router is Netbooting with a Token Ring connector, enter the following command to display the information about the connector, where <*connector*> is the connector number:

  get wfTokenRingEntry.*.1.<*connector*>

Identifying Remote Connectivity Problems

The sections that follow provide guidelines for isolating a router addressing problem or a Netboot problem. Refer to the appropriate section.

- Displaying Messages from the AN/ANH/ARN Console
- Displaying Statistics and Error Messages
- Guidelines for Using Packet Capture
- Guidelines for Using a LAN Protocol Analyzer

Displaying Messages from the AN/ANH/ARN Console

If you cannot connect to the router using Site Manager, we recommend that you connect the router to a modem or console.

If you cable the router to a modem, you can dial in and connect to the router remotely. This setup provides the same capabilities as an on-site console connection. Modem communications, however, are slower.

Viewing an AN/ANH/ARN error message and entering commands through a modem connection may simplify troubleshooting if you are not at the AN/ANH/ARN site. As an alternative, you can ask the person at the AN/ANH/ARN site to read the console messages to you and then you can enter the commands you want.

Displaying Statistics and Error Messages

Use the Statistics Manager Quick Get tool or the Technician Interface **get** command to display the number of BOOTP and TFTP packets forwarded and dropped for each interface in the path between the AN/ANH/ARN and the BOOTP server. Use the Events Manager tool or the Technician Interface **log** command to display the events associated with the interface and the BOOTP and TFTP protocols.

Refer to *Managing Routers* for instructions on using the Statistics Manager's Quick Get tool and the Events Manager. Refer to *Event Messages for Routers and BNX Platforms* for a description of events that appear in the log. Refer to *Using Technician Interface Software* for instructions on using the **get** and **log** commands.

Guidelines for Using Packet Capture

Use the Packet Capture utility to view incoming or outgoing BOOTP or TFTP packets and isolate errors to a specific router interface. This utility is available through the Technician Interface on routers running Version 7.80 or later.

Refer to *Using Technician Interface Software* for instructions on how to use Packet Capture. Refer to *Configuring SNMP, BOOTP, DHCP, and RARP Services* for a description of BOOTP packets.

Note: The instructions that follow assume that Version 7.80 or later is running on all routers in the path between the AN/ANH/ARN and the BOOTP server.

Use Packet Capture as follows:

1. **Test the BOOTP server's next-hop router in the path to the AN/ANH/ARN.**
2. **Test the upstream router's interface to the AN/ANH/ARN.**
3. **Test the upstream router's interface to the next-hop router.**
4. **Test the interfaces that receive and forward the BOOTP and TFTP packets of the router in the middle of the path.**
5. **Continue testing each router in the path until you isolate the problem interface.**

Guidelines for Using a LAN Protocol Analyzer

Refer to the following guidelines when you use a LAN protocol analyzer:

- If Netboot is failing, connect the analyzer to the BOOTP server interface to determine whether it is receiving and responding to Netboot and TFTP requests.

  To read the ASCII translation, view the BOOTP reply packets for the configuration file pathname in hexadecimal mode.

Note: The LAN protocol analyzer does not decode all of the vendor tag fields.

- If the BOOTP server is not receiving the requests, make sure that the upstream router is receiving and forwarding them. If it is receiving, verify that each router interface between the upstream router and the BOOTP server is receiving and forwarding them.

  If the BOOTP server is receiving requests, but failing to respond, refer to "Router Fails to Netboot" earlier in this appendix.

Resolving Connectivity Problems

This section describes how to

- Display the router's Netboot parameter settings.
- Debug the BOOTP server.
- Verify the BOOTP server's setup.
- Display the BOOTP server's IP routes.
- Display the number of BOOTP packets forwarded and dropped.

Displaying Parameter Settings

Display the router parameter settings to determine

- Whether the AN/ANH/ARN is set to boot using a local boot image or a remote boot image
- Whether the AN/ANH/ARN is set to configure using a local configuration file or a remote configuration file
- The configuration of the synchronous,Ethernet, and Token Ring (ARN only) connectors

Enter the following Technician Interface command to display the AN/ANH/ARN startup options:

getcfg

The following sample response shows the default settings for an AN or ANH with one Ethernet and two synchronous interfaces:

```
Boot Options

    boot image=local
    boot config=network

Netboot Parameters:

    XCVR1..None
    COM1...EZ-Install
    COM2...EZ-Install
```

The following sample response shows the settings for an ARN with one Ethernet, one Token Ring, and five synchronous interfaces:

```
Boot Options

    boot image=local
    boot config=network

Netboot Parameters:

    MAU1...None
    XCVR2..None
    COM1...EZ-Install
    COM2...EZ-Install
    COM3...EZ-Install
    COM4...EZ-Install
    COM5...EZ-Install
```

The possible `boot image` and `boot config` settings are `network` and `local`. If the setting is `network`, the AN/ANH/ARN requests the boot image or configuration file from a BOOTP server when booting. If the setting is `local`, the AN/ANH/ARN uses the boot image or configuration file stored in the Flash card file system.

The `XCVR` parameter shows the current setting of the Ethernet connectors. The `COM` parameters show the current settings of the synchronous connectors. The MAU parameter shows the setting of the Token Ring connectors (on ARNs only).

The possible settings for synchronous connectors are as follows:

- EZ-Install (the default setting)
- The IP address, next-hop IP address, subnet mask, and WAN protocol (Bay Networks HDLC or Frame Relay)

The possible settings for Ethernet connectors are as follows:

- `None` (the default setting)
- The IP address with subnet mask and next-hop IP address (if you configured one)

The possible settings for Token Ring connectors are as follows:

- `None` (the default setting)
- The IP address with subnet mask, ring speed option, and next-hop address (if you configured one)

See Chapter 5 for instructions on using the **ifconfig** and **bconfig** commands to change the parameter settings.

Debugging the BOOTP Server

Debug the BOOTP server as follows:

1. **Enter the following command at the UNIX command line:**

   bootpd -d -d&

   The *bootpd* debugger tool reads the */etc/bootptab* file and generates the */etc/bootpd.dmp* file. The */etc/bootpd.dmp* file contains the portion of the */etc/bootptab* file that the *bootpd* debugger could read successfully. The debugger displays messages such as the following:

   ```
   [1] 12914

      hostname:/etc> reading "/etc/bootptab"
      read 19 entries from "/etc/bootptab"
      dumped 19 entries to "/etc/bootpd.dump".
   ```

2. **Compare the** *bootptab* **file with the** *bootpd.dmp* **file.**

   If the *bootpd.dmp* file is truncated or is otherwise different from the *bootptab* file, BOOTPD may have encountered a syntax error. Find the inconsistency in the two files.

3. **Compare the inconsistency in the *bootptab* file to the sample *bootptab* file in Chapter 3 (refer to Figure 3-1) and correct the error.**
4. **If you cannot find an inconsistency, boot the router and view the *bootpd* debugger messages to determine the cause of the error.**

The sample messages in Table A-1 show the sequence of messages when a BOOTP exchange is successful.

Table A-1. BOOTP Messages

Message	Explanation
`hostname:/etc> request from IP addr 192.16.24.12`	The UNIX hostname, the path (*/etc*) of the *bootptab* file, and the IP address of the AN.
`found 192.16.24.12 AN.Boston`	The IP address (192.16.24.12) mapped to the hostname, AN.Boston, in the *bootptab* file.
`bootfile2 /$HOME/.builder_dir/rel812/an krnl_an.exe`	The pathname of the kernel file, as specified in the *bootptab* file.
`Couldn't access /$HOME/.builder_dir/rel812/an krnl_an.exe.AN.Boston`	Disregard this message. The BOOTP server tries to access the host both by its name and by its IP address. The “couldn’t access” message means that the server tried to access a host named “AN.Boston” but failed because the AN is not named. The attempt to access the AN by its IP address succeeds, as you can infer from the last message.
`vendor magic field is 99.130.83.99`	Disregard this message.
`sending RFC1048-style reply`	The BOOTP server is sending a BOOTP response in compliance with RFC 1048.

Verifying the BOOTP Server Setup

Refer to these instructions if the BOOTP server is receiving BOOTP requests but failing to respond, or failing to forward the kernel, configuration, application, or string files.

Verify the BOOTP server setup as follows:

1. **Make sure that the kernel image and all of the application (*.exe*) files are in the same directory.**

   You can place these files in any directory you want. The Image Builder automatically generates the kernel image and application files when you open the software image file. By default, the Image Builder stores these files for an AN/ANH in the */$HOME/.builder_dir/rel<rel>/an* directory, where *<rel>* is the current router software release for the AN/ANH. The default directory for the an ARN is */$HOME/.builder_dir/rel<rel>/arn*, where *<rel>* is the current router software release for the ARN.

   For example, Version 5.0 of the Site Manager's Image Builder tool stores the Version 11.0 files for an ARN in the */$HOME/.builder_dir/rel11.00/arn* directory.

2. **Make sure that the router extracts the kernel image and all of the application and string files from the same software image.**

   If these files are from different software versions, the router may fail to boot or may not operate properly.

3. **Make sure that the *bootptab* file is in the */etc* directory.**

4. **Make sure that the *bootptab* file for an AN/ANH contains the following entries:**

   ```
   general:\
       :hd=/$HOME/.builder_dir/rel<rel>/an:\
       :bf=krnl_an.exe:\
       :bs=auto:\
       :vm=rfc1048:
   ```

   The *bootptab* **file for an ARN should contain these entries:**

   ```
   general:\
       :hd=/$HOME/.builder_dir/rel<rel>/arn:\
       :bf=krnl_arn.exe:\
       :bs=auto:\
       :vm=rfc1048:
   ```

   Note that `/$HOME/.builder_dir/rel<rel>/an` is the default location of the kernel and all application and string files for the AN/ANH. The default location of the kernel and all application and string files for the ARN is `/$HOME/.builder_dir/rel<rel>/arn.`

5. **Make sure that the *bootptab* file contains a definition for the particular router that is failing to Netboot.**

6. **Make sure that the configuration filename and path are correct in the *bootptab* file.**

   For example, the following *bootptab* line indicates that the configuration file named *AN_Bost.cfg* is in the */rte3/cfg* directory path:

   ```
   T129="/rte3/cfg/AN_Bost.cfg"
   ```

7. **Read the *bootptab* file carefully for misspellings or other errors.**

   Compare it to the sample file shown in Chapter 3 (refer to Figure 3-1).

Displaying the BOOTP Server's IP Routes

Enter the following command at the UNIX command line of the BOOTP server to display the IP address of the next hop to a netbooting router:

netstat -rn | grep -i -n *<IP_address>*

<IP_address> is the IP address of the netbooting router's network.
| is the vertical bar key (the UNIX pipe command).

For example, enter **netstat -rn | grep -i -n 192.32.155** to display the IP address of the next hop to the network address 192.32.155.

If the BOOTP server is receiving RIP advertisements of the netbooting router's network, a message such as the following appears:

```
121:192.32.155.0    192.32.13.53   UG   0   0   le0
```

The number `121` is the number of the entry in the workstation's static routing table. The number `192.32.155.0` is the IP address of the destination network. The number `192.32.13.53` is the address of the next-hop router. If the next-hop router is unavailable or wrong, refer to "Setting Up Static Routes to Next-Hop Routers" in Chapter 3.

Displaying the Number of Packets Forwarded and Dropped

This section describes how to display the number of BOOTP packets forwarded and dropped by a router. Perform this procedure for each router between the router and the BOOTP server.

You can use either the Quick Get function of the Statistics Manager tool or the Technician Interface **get** command to retrieve this information. Refer to *Managing Routers and BNX Platforms* for additional information about Quick Get.

Quick Get Instructions

1. **Select the following path:**

   `wfApplication/wfInternet/wfBootpGroup/wfBootpRelayAgentGroup/wfBootpRelayIntfTable`

2. **To display the number of packets forwarded, select**

   `wfBootpRelayIntfRequests`

3. **To display the number of packets dropped, select**

   `wfBootpRelayIntfHopsDrops`

Technician Interface Instructions

Enter the following command to display information that may help you determine if and why a device is dropping packets, where *<IP_address>* is the address of the interface receiving the packets:

get wfBootpRelayIntfEntry.*.*<IP_address>***

Maintaining the Router Software

The AN/ANH/ARN file system resides on the Flash memory card. This part of the router is *not* user-serviceable.

You use Technician Interface commands to maintain the local file system on the AN/ANH/ARN Flash card. See *Using Technician Interface Software* and *Using Technician Interface Scripts* for information.

Caution: Be very careful when you use the **format** command with the router. This command erases all files on the local Flash card, and the router will not be able to local-boot an image or configuration file until you replace the files. You can avoid this situation by partitioning the Flash card media. See *Using Technician Interface Software* and *Managing Routers and BNX Platforms*.

When Technician Interface commands require you to specify a volume, always specify Volume 1 for an AN/ANH/ARN.

Upgrading the Software Image

You can upgrade an AN/ANH/ARN's software image (*krnl_an.exe* for the AN/ANH or *krnl_arn.exe* for the ARN) using one or both of the following options:

- Use Netboot to start the router.

  This option upgrades the image only in the router's RAM.

- Use TFTP to transfer the image to the router's local file system, and then use Local Boot to start the router.

  This option upgrades the image in both the router's local file system and in memory.

Caution: If you use TFTP to transfer an upgraded image to an AN/ANH/ARN Flash card, and an interruption in the file transfer occurs (for example, if the router resets, reboots, or loses power), the router's local file system becomes corrupted and it cannot boot locally until the file system is restored.

Restoring a Local File System

If the local file system becomes corrupted, you must restore it by upgrading the software image.

If for any reason the router resets, reboots, or loses power while restoring or compacting its Flash card file system, it automatically Netboots the configuration file and software image. (You must already have the network set up for Netboot to succeed.)

Note: On AN models, if the router reboots while it is writing to or compacting *partitioned* Flash memory, the file system becomes corrupted. As a result, the router will not start after rebooting.

After the router successfully Netboots, you can use TFTP to restore the software image and configuration file on the local file system.

Caution: Compacting the file system on a Flash card can take up to 15 minutes. When you compact a router's file system, always let compaction complete before you reset the router.

Appendix B
Using the Local Boot Procedure

If you have read Chapter 2 and want to use the Local Boot (Quick-Start) process to start an AN, ANH, or ARN for the first time, use the information and worksheets in this appendix to gather the network information required to complete the procedure.

Note: The worksheets in this appendix apply only to AN, ANH, and ARN models. See *Quick-Starting Routers* for all other Bay Networks routers.

The last section in this appendix, "Running the Quick-Start Script," provides information about the Local Boot startup procedure.

What Is Quick-Start?

The Quick-Start procedure is the initial configuration that

- Enables Internet Protocol (IP) so that the router can connect to Site Manager
- Starts a locally booted router running on the network

You perform the procedure by running the *install.bat* script (for Quick-Starting AN and ANH models) or the *inst_arn.bat* script (for ARN models), and entering information at the prompts. The router automatically selects options for some prompts, and you can accept default values for many of the other prompts.

Note: The Quick-Start procedure for ARN models is nearly identical to the procedure for AN/ANH models; however, this Appendix identifies any differences.

Using the Worksheets

This appendix includes a series of worksheets to help you organize the network information you need for your specific configuration and to answer Quick-Start prompts. The worksheets contain the options for each prompt and provide space for you to record the options you select.

Note: The *install.bat* and *inst_arn.bat* scripts allow for many possible configurations. Since typical remote access uses a serial interface over a wide area connection, the following worksheets provide only the options involved with a serial configuration. When you configure a LAN interface, base your decisions on the information provided with each *install.bat* or *inst_arn.bat* prompt.

If you are not configuring the router yourself, fill out the worksheets for a person at the router site and relay the worksheet information. Written for a person at the router site, the manuals *Installing and Operating BayStack AN and ANH Systems* and *Installing and Operating BayStack ARN Routers* include identical worksheets and instructions for completing the Quick-Start procedure.

Prepare for the procedure as follows:

1. **Fill out the Global Information Worksheet completely.**

   This worksheet lists options common to all synchronous interface configurations.

2. **After you record your protocol selections on the Global Information Worksheet, fill out *one* Router Protocol worksheet.**

   This worksheet lists specific options for RIP, OSPF, or Static Route configurations. For example, if you select RIP as your routing protocol, you need to fill out only the worksheet pertaining to RIP.

3. **Fill out *one* Wide Area Protocol worksheet.**

   This worksheet lists specific options for Bay Networks (proprietary) Point-to-Point Protocol (PPP), Frame Relay, Standard PPP, and Switched Multimegabit Data Service (SMDS) configurations. For example, if you select Frame Relay as your wide area protocol, you need to fill out only the Frame Relay worksheet.

4. **Run *install.bat* or *inst_arn.bat* as described in "Running the Quick-Start Script" later in this chapter.**

Or, a remote-site operator runs the installation script as described in the hardware installation guide.

5. **Once the router has an initial connection to the network, use the guide** *Configuring Routers* **to configure the router using Site Manager.**

Global Information Worksheet

This section contains the prompts and options relating to all AN/ANH/ARN synchronous configurations. Write your selection in the "Your Response" column.

Global Information Worksheet

Step	Requested Information	Options	Your Response
1	**AN/ANH only:** Specify the slot number where the Link Module resides.	Because the AN/ANH is not a Link Module, the router bypasses this step and automatically accepts a default slot of "1."	None.
	ARN only: Enter the module number [1]:	The script lists the available modules that you can use to connect the router's IP network interface to Site Manager. For example, the script might offer the following options: 1. ARNMBSTR (Token Ring on Motherboard) 2. ARNSSYNC (Sync on Serial Daughterboard 1) 3. ARNENTSYNC (Ethernet Tri-Sync on Expansion Module)	Enter the number that corresponds to the module you want to use.
2	Driver Type:	If there is only one interface on the module you chose, the script automatically selects the driver type for that interface and bypasses this prompt. Otherwise, the script displays a menu of driver types. The actual menu depends on the modules you have installed.	Choose the Synchronous driver.

(continued)

Global Information Worksheet *(continued)*

Step	Requested Information	Options	Your Response
	Enter connector number [1]:	If there is only one connetor on the module you chose, the script automatically assigns a connector number and bypasses this prompt. Otherwise, the script lists the available connectors. For example, for an ARN with five synchronousconnectors, the options are 1. COM1 2. COM2 3. COM3 4. COM4 5. COM5	
	Enter clock source number [2]:	1. Internal 2. External	
	Enter clock speed number [10]:	This prompt appears only if you chose an Internal clock source. The script lists a range of values, with 64 K as the default.	
	Enter circuit name [S#]:	The script displays a default circuit name for the COM interface you selected (for example, S11 for COM1 and S12 for COM2).	Press the Return key.

(continued)

Global Information Worksheet *(continued)*

Step	Requested Information	Options	Your Response
3	Enter IP address in dotted decimal notation:	Enter the IP address for the COM interface.	
	Enter IP subnetwork mask in dotted decimal notation:	Enter the subnetwork mask for the COM interface IP address.	
	Is the router connected to the same local area network as the Site Manager workstation? (y/n) [n]:	y(es) n(o)	Press the Return key.
	Enter routing protocol number [1]:	1. RIP 2. OSPF 3. Static Route to Site Manager	(Complete the worksheet for the protocol you select.)
	Enter wide area protocol number [1]:	1. Bay Networks Point-to-Point Protocol (Proprietary) 2. Frame Relay 3. Point-to-Point Protocol (PPP) Standard 4. Switched Multimegabit Data Service (SMDS)	(Complete the worksheet for the protocol you select.)
	Do you wish to set SNMP community management? (y/n) [n]:	y(es) n(o) Setting up SNMP community management is optional.	
4	Enter (TFTP) volume number [1]:	The script automatically selects “1” as the TFTP default volume.	None
5	Do you want to enable FTP? (y/n) [n]:	y(es) n(o) Enabling FTP is optional.	
	Enter (FTP) volume number [1]:	The script automatically selects “1” as the FTP default volume.	

(continued)

Global Information Worksheet *(continued)*

Step	Requested Information	Options	Your Response
6	Do you want to enable TI TELNET (y/n) [n]:	y(es) n(o) Enabling TELNET is optional.	
7	Do you wish to save this configuration to a file? (y/n) [y]	y(es) n(o)	Press the Return key.
	Enter filename [*startup.cfg*]:	We recommend using the default filename.	Press the Return key.
	ARN only: Do you wish to set up another port/module? (y/n) [y]	y(es) n(o)	Type **n** and press the Return key.

Router Protocol Worksheets

This section contains requested information and possible options relating to the routing protocol choices on the Global Worksheet.

RIP Worksheet

Requested Information	Options	Your Response
Should RIP listen to the default route? (y/n) [n]:	y(es) n(o) **Note:** RIP listens to a specific network or subnet route where Site Manager is located. Answering y(es) to this request forces RIP to also listen to the default route (0.0.0.0). This is useful when no specific route is available in the RIP updates that the router receives.	

OSPF Worksheet

Requested Information	Options	Your Response
Enter OSPF router ID in dotted decimal notation:	Enter an IP address to uniquely identify the router in the OSPF domain. The router provides the IP address of the COM port. We suggest using the default IP address.	
Enter the OSPF area ID in dotted decimal notation [0.0.0.0]:	Enter the area ID. This ID must match the area ID of the router's neighbor. **Note:** The backbone area ID is always 0.0.0.0.	
Enable Simple Password authentication? (y/n) [n]:	y(es) n(o) **Note:** If you answer y(es), the router requests a password.	Password: _____
Follow default paths for unknown subnets? (y/n) [n]:	y(es) n(o)	
Enter OSPF MTU size selection [1]:	1. Default 2. Ethernet size (Bay Networks Series 5 compatible) 3. User Defined MTU	

(continued)

OSPF Worksheet *(continued)*

Requested Information	Options	Your Response
Enter OSPF interface type selection [1]:	1. Broadcast 2. NBMA 3. Point-to-Point 4. Point-to-Multipoint (Proprietary) 5. Point-to-Multipoint (Per OSPF Standard) **Note:** When using a wide area protocol other than Bay Networks Proprietary PPP, we suggest selecting NBMA.	
Enter decimal value in seconds for Hello Interval [10]: **Note:** This value must match all other interfaces in the OSPF area for connection to take place.	The script suggests the following intervals: Broadcast -- 10 seconds Point-to-Point -- 15 seconds NBMA -- 20 seconds Point-to-MultiPoint --10 seconds	
Enter decimal value in seconds for Router Dead Interval [40]: **Note:** This value must match all other interfaces in the OSPF area for connection to take place.	The script suggests the following intervals: Broadcast -- 40 seconds Point-to-Point -- 60 seconds NBMA -- 80 seconds Point-to-MultiPoint (STD) -- 40 seconds	
Enter decimal value for Router Priority [1]: (For Broadcast, NBMA, or Point-to-MultiPoint)	Enter a router priority value. The lower the value (above zero), the higher the priority. **Note:** If you set the router priority to zero (0), the router is not eligible to become the designated router on this network.	

(continued)

OSPF Worksheet *(continued)*

Requested Information	Options	Your Response
Enter decimal value in seconds for Poll Interval [20]: (For NBMA only)	Enter the largest number of seconds allowed between Hello packets that the router sends to an inactive NBMA neighbor. The router suggests a 20-second interval.	
Enter IP address of neighbor in dotted decimal notation or enter **q** to quit: (For NBMA only)	Enter addresses for all NBMA neighbors you want the router to communicate with. Enter **q** and press the Return key when you finish entering addresses.	
Enter IP address of neighbor in dotted decimal notation: (For PPP only)	Enter addresses for the PPP neighbor you want the router to communicate with.	

Static Route to Site Manager Worksheet

Requested Information	Options	Your Response
Destination Network [0.0.0.0]:	Enter the gateway address of the destination network. An address of 0.0.0.0 specifies the default route.	
Destination Network Mask [0.0.0.0]:	Enter the subnetwork mask of the destination network. A mask of 0.0.0.0 specifies the default route.	
Next-Hop Address:	Enter a next-hop address. All static routes require a next-hop address in the same subnet as the initial IP interface.	

(continued)

Static Route to Site Manager Worksheet *(continued)*

Requested Information	Options	Your Response
Follow the default route for unknown subnets? (y/n) [n]:	y(es) n(o) The default route does not apply for subnets unless you enter **y** at this prompt.	

Wide Area Protocol Worksheets

This section contains requested information and possible options relating to wide area protocol choices on the Global Worksheet.

Bay Networks Proprietary PPP Worksheet

Requested Information	Options	Your Response
Enter BofL (Breath of Life) timer value (1-60) [5]:	Enter the maximum amount of time that can elapse between the successful transmission of BofL messages.	
Enter Local Address selection [3]:	1. DCE 2. DTE 3. EXPLICIT **Note:** Reverse local and remote address values when configuring the device at the other end of the circuit. (Exception: When connecting to a Series 5 router that uses DCE/DTE addressing, use the SAME local address value.)	

(continued)

Bay Networks Proprietary PPP Worksheet *(continued)*

Requested Information	Options	Your Response
Enter Remote Address selection [3]:	1. DCE 2. DTE 3. EXPLICIT **Note:** Reverse local and remote address values when configuring the device at the other end of the circuit. (Exception: When connecting to a Series 5 router that uses DCE/DTE addressing, use the SAME local address value.)	

Frame Relay Worksheet

Requested Information	Options	Your Response
Enter Management type [3]:	1. DLCMI None 2. Rev 1 LMI 3. ANSI T1 617D 4. CCITT Annex A 5. LMI Switch 6. Annex D Switch 7. Annex A Switch	
Enter addressing type [4]:	1. ADDR Q.921 2. ADDR Q.922 (MARCH '90) 3. ADDR Q.922 (NOVEMBER '90) 4. ADDR Q.922	
Enter address field length [2]:	2. Two Bytes 3. Three Bytes 4. Four Bytes	
Enter DLCI number [30]: (For DLCMI None, LMI Switch, Annex D Switch, and Annex A Switch only)	Enter the Permanent Virtual Channel (PVC) number. **Note:** The valid range for the DLCI number is between 16 and 1007.	

PPP Standard Worksheet

Requested Information	Options	Your Response
Enter Remote IP address in dotted decimal notation:	Enter the IP address of the peer connection.	
Do you wish to turn on the PPP echo function? (y/n) [n]:	y(es) n(o)	
Enable PAP (Password Authentication Protocol)? (y/n) [n]:	y(es) n(o) **Note:** If you answer y(es), the router requests a PAP ID and password for this interface. If you answer n(o), the router asks whether you want to enable CHAP.	
Enable CHAP (Challenge Handshake Authentication Protocol)? (y/n) [n]:	y(es) n(o) **Note:** If you answer y(es), the router requests a CHAP secret for this interface.	
Does the Remote Peer have PAP authentication enabled? (y/n) [n]:	y(es) n(o) **Note:** If you answer y(es), the router requests the PAP ID and password for the remote interface.	
Enable the LQR (Link Quality Reporting) Protocol? (y/n) [n]:	y(es) n(o) **Note:** Link Quality Monitoring on a Bay Networks Series 5 router is not compatible with this feature.	

(continued)

PPP Standard Worksheet *(continued)*

Requested Information	Options	Your Response
Enable use of the Remote Peer router's LQR Timer? (y/n) [y]: (For LQR Protocol only)	y(es) n(o) **Note:** If the LQR timer is enabled, the remote peer router maintains its own LQR timer for this interface. When the LQR timer is disabled, the AN is responsible for maintaining the timer for this interface.	
Number of seconds (1-120) [3]: (For LQR Protocol only)	Enter the maximum number of seconds between the transmission of LQR packets.	
Enter [inbound] success rate percentage (1-100) [90]:	Enter the minimal acceptable success rate (percentage) of packets transmitted by the peer router and received on this interface over the last 5 LQR reporting periods.	
Enter [outbound] success rate percentage (1-100) [90]:	Enter the minimal acceptable success rate (percentage) of packets transmitted by this interface and received by the peer router over the last 5 LQR reporting periods.	

SMDS Worksheet

Requested Information	Options	Your Response
Enter 10-digit individual address:	Enter the individual address assigned to you by your SMDS service provider.	
Enter 10-digit group address:	Enter the group address assigned to you by your SMDS service provider.	
Enter 10-digit arp address:	Enter the Address Resolution Protocol (ARP) address assigned to you by your SMDS service provider.	

Running the Quick-Start Script

You run the *install.bat* or *inst_arn.bat* script as part of the Local Boot process. Begin Local Boot as follows:

1. **At the Technician Interface `login:` prompt, enter Manager to log in.**

   Be sure to have the completed worksheets with you.

2. **Enter bconfig config local to configure the router to use the local *config* file when booting.**

   For information about the **bconfig** command, see "Configuring the Router Boot Source" in Chapter 5.

3. **Reboot the router by entering boot.**

   The Technician Interface login prompt appears.

4. **Log in to the Technician Interface.**

   The Technician Interface mounts the local file system and displays a prompt indicating the present working directory.

5. **Do one of the following:**

   - To run the Quick-Start procedure for AN and ANH models, enter the following command:

     run install.bat

   - To run the Quick-Start procedure for ARN models, enter the following command:

     run inst_arn.bat

6. **Follow the script online, using your worksheets for responses to its prompts.**

   Refer to the list of commands in Table B-1.

Table B-1. Quick-Start/Power-Start Commands

To Do the Following	Action	Details
Accept a default value	Press return	Your console displays default values in brackets; for example, [E11].
Repeat a step (for example, if you make a mistake)	Press **Control-c** Press **n**	When prompted, “Terminate script y/n?” press the **n** key. You return to the beginning of the step so you can reenter the information.
Stop the Quick-Start installation procedure	Press **Control-c** Press **y**	When prompted, “Terminate script y/n?” press the **y** key. The procedure is terminated and you return to the Technician Interface prompt. To restart the Quick-Start/Power-Start procedure, you must reboot the router by entering **boot**.

The script prompts you for the following information (in the order given):

a. The initial Global Worksheet information

b. Specific protocol information

c. Wide area protocol selection

d. Specific protocol information

e. The rest of the Global Worksheet information

After you enter all of the Global Worksheet protocol information, the script displays a Configuration Summary and prompts you to save the configuration to a file.

7. **Name and save the configuration file.**

The script begins to test the configuration on the new IP interface (Figure B-1).

```
Testing local IP interface

ping -IP 192.32.00.000 -r5
IP ping:  192.32.00.000 is alive (size - 16 bytes)
IP ping:  192.32.00.000 is alive (size - 16 bytes)
IP ping:  192.32.00.000 is alive (size - 16 bytes)
IP ping:  192.32.00.000 is alive (size - 16 bytes)
IP ping:  192.32.00.000 is alive (size - 16 bytes)


This test attempts to ping the Site Manager workstation.

NOTE: If routing has not yet converged, an attempt
       to ping the Site Manager workstation may fail.  If
       this happens, you may either enter a new IP address or
       quit and wait a short period of time and try again from
       the TI command line.

Type q<return> to cancel this test.

Enter IP address of Site Manager workstation:
```

Figure B-1. Starting the IP Interface Test

8. **To continue the IP configuration test, enter the IP address for the Site Manager workstation.**

   To cancel the test, enter **q**.

9. **On ARN models, choose whether you want to configure another module/port.**

   If you enter **n**, (to stop configuring modules/ports), the Technician Interface prompt appears. If you enter **y**, you return to Step 6 of this procedure.

10. **When the Technician Interface prompt reappears, enter logout to exit the Technician Interface.**

Once the router creates and tests the configuration, it starts using the configuration information you entered. Refer to *Configuring Routers* to configure the router using Site Manager.

Appendix C
Implementation Notes

This appendix contains implementation hints, a few important notes you could have missed earlier in this guide, and guidelines for planning AN/ANH/ARN network configurations.

Hints

This section contains a few hints for setting up an AN, ANH, or ARN.

- We recommend that you first install an AN/ANH/ARN in the same site as your BOOTP server, Site Manager workstation, and intermediate Bay Networks routers to test the software image, configuration file, and routing path. This test provides you with the startup and troubleshooting experience you need to perform these tasks on routers at remote sites. After you perform the test, move the test router to the remote location you want, modify the configuration file for that router, and set up the new paths.
- After you build and test the remote router configuration file, make copies of it on the Site Manager workstation. Then modify the copies for each AN/ANH/ARN in your network, rather than starting over. To avoid mix-ups, make sure that the filename you assign to each configuration file is unique and meaningful for each router.
- It may be easier to isolate BOOTP and TFTP configuration errors on the network if you upgrade all Bay Networks routers in the paths between the routers and the BOOTP server to Version 7.80 or later before you set up the paths.

- If you are using EZ-Install over Frame Relay to boot an AN/ANH/ARN, you can have up to 20 PVCs for a single Frame Relay interface on the upstream router. If you have more than 20 PVCs on the interface where EZ-Install is occurring, the EZ-Install process may fail. To ensure that the process does not fail, configure no more than 20 PVCs for a Frame Relay interface.
- If the AN/ANH/ARN will have small routing or forwarding tables, you can increase performance by reducing local memory and allocating more global memory for buffers. If the router will have large tables (for example, more than 500 servers), you might want to increase the local memory allocation.

Notes

- If you use TFTP to transfer the software image file to upgrade or restore the router's file system, be sure to specify the router's image (*an.exe* for the AN/ANH or *arn.exe* for the ARN).
- Bay Networks supports BOOTP service on UNIX workstations, but not PCs. If you want to use Netboot and you are using a PC as your Site Manager workstation, transfer the files you want to Netboot from the PC to a UNIX workstation and configure the workstation as a BOOTP server.
- On an AN/ANH/ARN, you cannot use EZ-Install or Netboot directly from a FDDI interface. On an AN/ANH, you cannot use EZ-Install or Netboot directly from a Token Ring interface.
- You need Version 8.10 or later to perform Directed Netboot.
- If you have a LAN protocol analyzer available, you may want to use it to troubleshoot BOOTP server communication errors. (Appendix A provides guidelines for using Packet Capture and an analyzer to isolate these errors.)
- Versions earlier than 7.80 do not include the Technician Interface Packet Capture utility.
- The 12-port ANH polls the internal repeater module for operation status; it does not poll individual Ethernet repeater ports for connection (link) status. Therefore, the 12-port ANH is aware of the connection between the base board and repeater module, but is not aware of any connection between the repeater module and the Ethernet network. If the repeater module interface state reports an operational status, the 12-port ANH may continue to transmit information through the repeater module even though a physical Ethernet connection does not exist.

- You can issue a **boot** command from the Diagnostic Monitor prompt and specify a local boot by using `1:` as the volume name.
- When at the diagnostic prompt, you cannot view the contents of Flash memory. Be extremely careful to remember the name of the configuration file when doing a named boot from the Diagnostic Monitor prompt.

Network Configuration Options

This section describes several options for configuring an ANH in a network. It provides general requirements and recommendations for network configurations using the ANH, as well as examples of valid configurations.

The basic configuration uses a standalone ANH in a departmental network (see the section "Configuring a Single ANH"). To accommodate more stations, you can connect (*daisy-chain*) multiple ANH systems (see the section "Configuring Multiple Hubs").

Note: The examples and illustrations in this section show the 8-port ANH, but they apply to any Bay Networks ANH system.

Ensuring Ethernet Network Compliance

Before configuring any network hardware, use the following rules to assess your network for compliance with Ethernet operating standards. Using these rules allows you to avoid performing the detailed calculations specified in the IEEE 802.3 specifications.

The network is compliant when it meets all of the following requirements:

- No path through the network contains more than five repeaters.
- No more than 1024 stations are connected (not counting repeaters).
- The entire Ethernet network consists of only IEEE 802.3 components, using only AUI, 10Base-T, FOIRL, 10Base-F, 10Base-5, or 10Base-2 cables.
- Fiber optic link attenuation limits are met. (Refer to the attenuation specifications for the fiber optic cable, connectors, and transceiver or device transmitter/receiver ports that you are using.)
- No link is longer than the IEEE 802.3 maximums, given in Table C-1.

Table C-1. IEEE 802.3 Maximum Segment Links

Segment Type	Maximum Segment Length (m)
10Base-5 (coaxial)	500
10Base-2 (coaxial)	185
10Base-T	100
10Base-FB	2000
10Base-FL	2000
FOIRL	1000
AUI drop	50 (2-m allowance + 48-m excess)

Network paths composed of three or four repeaters must also comply with the following additional restrictions.

Network Path Containing Three Repeaters

In the longest path containing three repeaters, no transmit-end or receive-end fiber link can be longer than 400 meters (m).

Network Path Containing Four Repeaters

In the longest path containing four repeaters:

- No more than three links are maximum-length coaxial segments.
- No fiber link is longer than 500 m; or if one or more is longer, the total of all fiber links does not exceed 2500 m (2740 m if all are 10Base-FB).

Configuring a Single ANH

The basic ANH configuration consists of one ANH, one local management console, and as many as nine 10Base-T devices in a standalone local area network configuration.

You can directly connect as many as eight 10Base-T Ethernet stations into a local Ethernet segment using a single 8-port ANH.

Note: You can add a ninth Ethernet station to the AUI port using a 10Base-T transceiver. The section “Configuring an AUI Port” describes other options for using the AUI port.

Figure C-1 shows an example of a single ANH network configuration. UTP distribution cables connect Ethernet stations that have either an installed 10Base-T network interface card (NIC) or an AUI NIC plus an external 10Base-T transceiver.

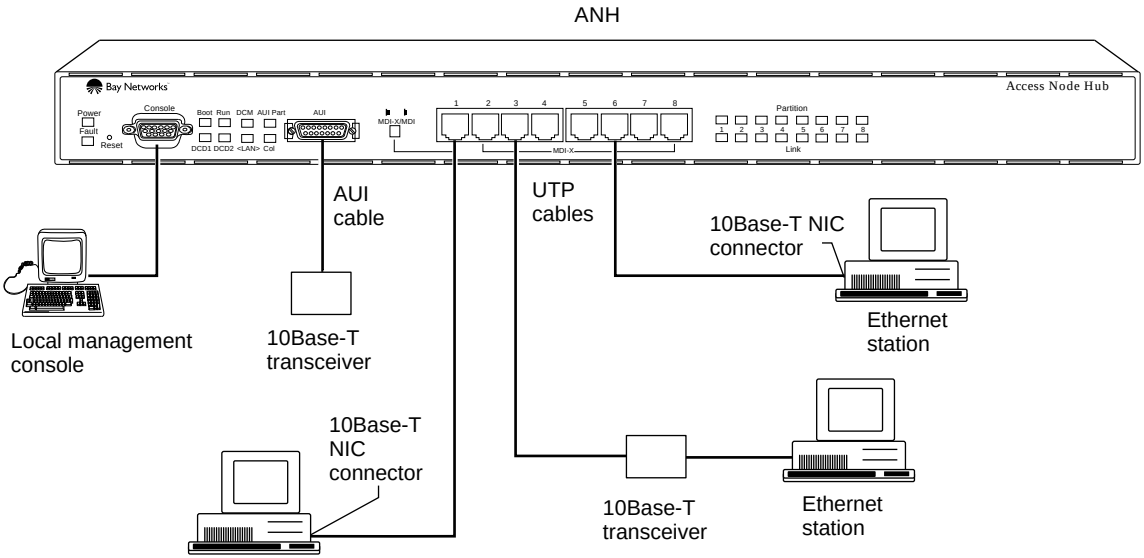

Figure C-1. Typical Single-ANH Configuration

Note: In Figure C-1, the local management station (directly connected through the console port) can be either an ASCII- or PC-based terminal. In larger network configurations, you can also connect the ANH to an SNMP management station through a 10Base-T repeater port (see Figure C-4).

Configuring Multiple Hubs

You can interconnect as many as four ANH units using the UTP repeater ports.

Note: Backbone connections are usually made through the AUI port (see the section “Configuring an AUI Port”).

When you configure a network with multiple ANH (or other repeater/hub) systems, you must comply with the following rules:

- Connect no more than four hubs.
- Make sure that each UTP connection is no longer than 100 m.
- If a transceiver is connected to the AUI port, disable the SQE (signal quality error) test function of the transceiver.

Note: Minimize the number of repeaters between stations in the network by connecting hubs in a star configuration. Avoid chaining hubs in a single line.

When connecting three or four hubs, make sure that the installation complies with the specifications in “Ensuring Ethernet Network Compliance” earlier in this chapter.

Figure C-2 shows an ANH linked with two Model 810M hubs. UTP patch cables connect each MDI port to an MDI-X port. For information about activating the MDI-X/MDI switch, see *Installing and Operating BayStack AN and ANH Systems*.

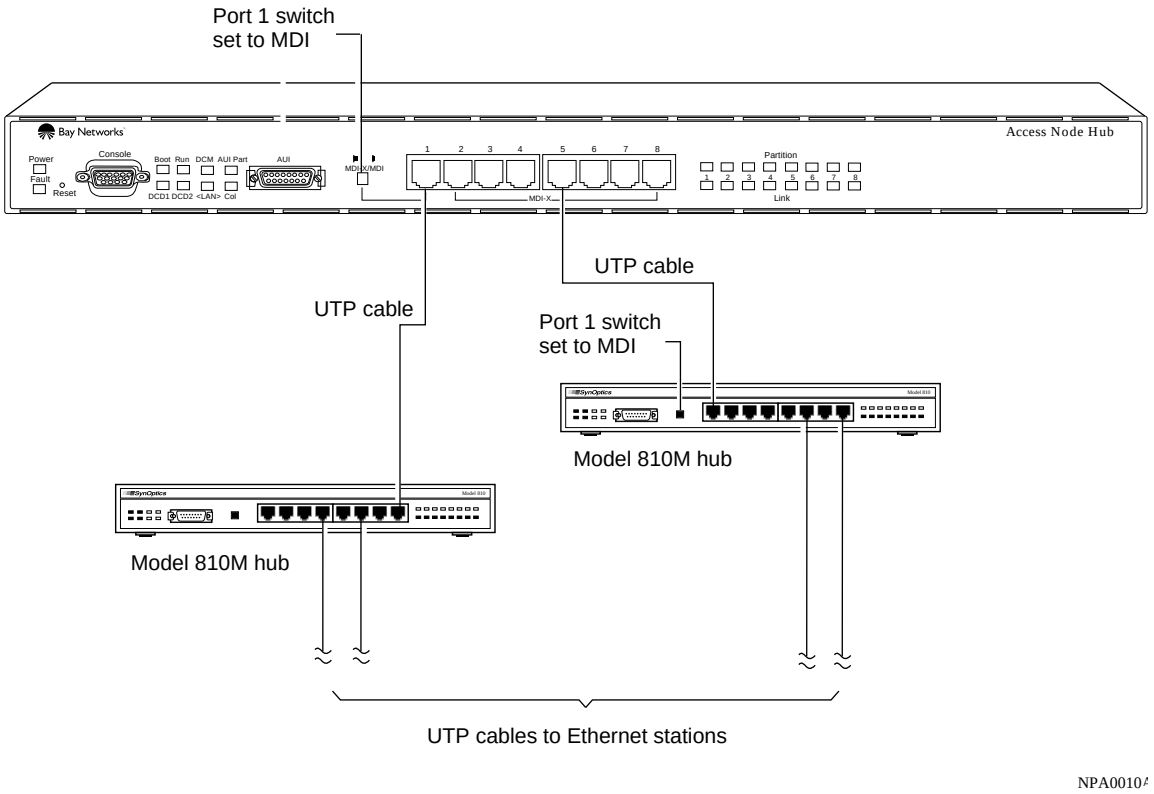

Figure C-2. Connecting the ANH with Other Hubs

Configuring an AUI Port

You can connect any IEEE 802.3 media attachment unit (MAU) to the AUI port on an AN or ANH. For example, you can use an IEEE 802.3 10Base-FL fiber optic MAU (FOMAU) to connect to a fiber optic port on a router or hub. Or, you can connect the AUI port to a coaxial backbone through an IEEE 802.3 10Base-5 or 10Base-2 MAU.

Caution: IEEE 802.3 rules require that the SQE test function be disabled on an IEEE 802.3 MAU connected to an AUI port. If it is not disabled, the AUI port could interrupt network transmissions until it *autopartitions* (automatically goes off-line after 32 consecutive collisions).

Connecting the AUI Port to a Fiber Optic Backbone

To connect an AN or ANH to a fiber optic backbone, you must first connect an IEEE 802.3 10Base-FL (or 10Base-FB) transceiver to the AUI port.

Figure C-3 shows an example network with two 8-port ANH systems connected via a fiber optic backbone. An AUI cable connects each ANH to a transceiver that has the SQE test function disabled. A fiber optic cable connects the two transceivers.

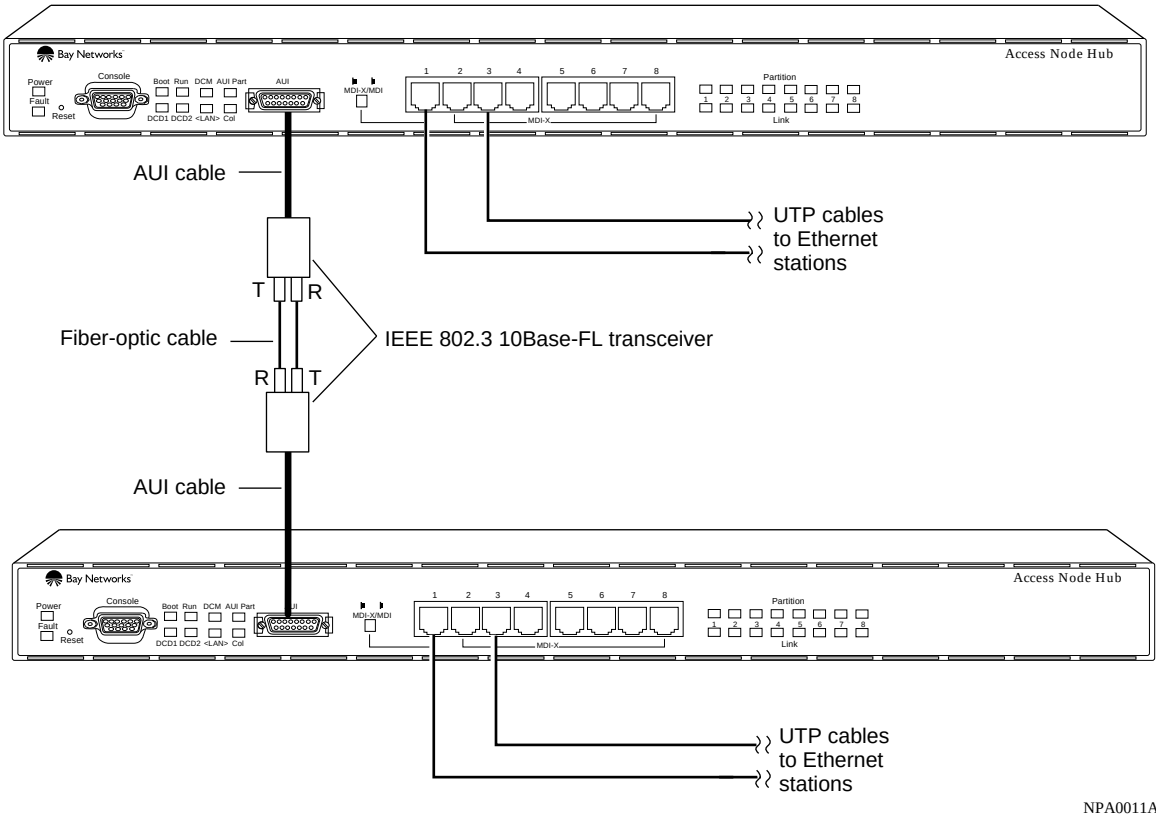

Figure C-3. Connecting Two ANH Systems Using 10Base-FL Transceivers

Connecting the AUI Port to a Coaxial Backbone

You can use the AUI port to connect an AN or ANH to a coaxial backbone through an IEEE 802.3 10Base-5 or 10Base-2 coaxial MAU.

Figure C-4 shows two ANH systems connected to a coaxial backbone through IEEE 802.3 MAUs. An AUI cable connects the AUI port on each ANH to each MAU. The SQE test is disabled on each MAU connected to the AUI port on an ANH.

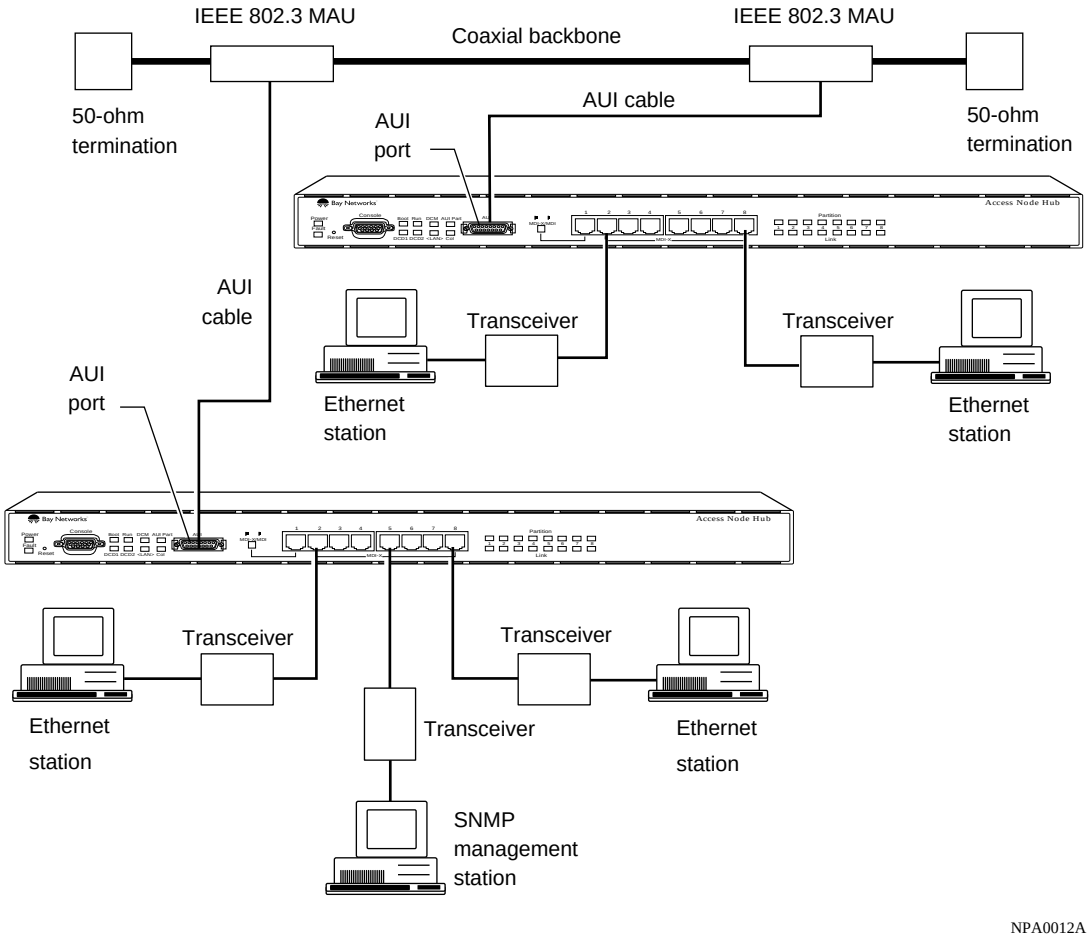

Figure C-4. Connecting ANH Systems through a Coaxial Backbone

Index

Symbols

/etc/inetd.conf file, 3-9, 3-10

/etc/services file, 3-2

/tftpboot directory, 3-10

/usr/wf/config directory, 3-3

A

address. *See* IP address

AIX operating system
- BOOTPD, 3-2
- TFTPD access, 3-10

Alarm group, 7-5, 7-23

an.exe file, 1-2, C-2

analyzing packets
- on a router, A-9
- on the BOOTP server, A-9

ANH
- 12-port
  - disabling, 6-3
  - port status, 6-3
  - status, C-2
  - thirteenth port, 6-3
- 8-port
  - AUI interface, 6-2
  - ninth port, 6-2
  - port status, 6-2
- AUI connections, C-5
- compliance rules, C-4
- configuring
  - in a network, C-3 to C-9
  - multiple, C-6
  - single, C-4
- enabling ports on, 6-1
- repeater ports
  - autopartitioning, C-7
  - enabling, 6-1
  - managing, 6-1
- resetting and testing, 6-4 to 6-5

application files
- definition, 1-2
- generating, 4-6

applications, troubleshooting, A-5

arn.exe file, 1-2, C-2

AUI connections
- ANH, C-5
- coaxial backbone, C-9
- disabling SQE test function, C-6
- examples, C-7 to C-9

automated addressing. *See* IP address

B

backbone
- coaxial, C-9
- fiber optic, C-8

base record, DCM, 7-15

Bay Networks
- CompuServe forum, xxx
- Customer Service FTP, xxix
- home page on World Wide Web, xxix
- InfoFACTS service, xxxi
- publications, ordering, xxv
- support programs, xxviii
- Support Source CD, xxx
- Technical Response Center, xxvii, xxxi
- technical support, xxvii

Bay Networks Proprietary PPP protocol, worksheet for, B-10
Bay Networks Standard PPP protocol, 5-5
Bay Networks Standard protocol, 4-21
bconfig command
  examples, 5-3
  format, 5-2
bf (boot file) tag, in bootptab file, 3-6
boot
  DCM board, 7-13
  failure, 1-3
  file tag, 3-6
  getcfg command display, 5-9, A-11
  process, 1-6
  size tag, 3-7
  while writing to a file, A-17
Boot Config From Network parameter, 4-9
Boot Config Pathname parameter, 4-10
Boot Image From Network parameter, 4-8
Boot Image Pathname parameter, 4-10
Boot Server Address parameter, 4-9
BOOTP
  analyzing packets on a router, A-9
  client interface table, 1-9, 4-21 to 4-23
  failure of, A-2
  pass-through, enabling, 4-16
  relay agent forwarding table, 4-17 to 4-20
  relay, enabling, 4-16
  setting up, 3-2 to 3-13
  Site Manager support, C-2
  socket, 3-2
  testing, C-1
BOOTP server
  analyzing packets, A-9
  debugging, A-12
  displaying IP routes, A-15
  location of files, 4-2
  not receiving BOOTP requests, A-4
  responses, failure of, A-2
  router software version, C-1
  troubleshooting, A-4, A-14
BOOTPD
  copying, 3-2
  debugger tool, A-12
  linking to TFTPD, 3-10
  send and receive sockets, 3-2
bootpd.dmp file, A-12
bootptab file
  debugging, A-13
  editing, 3-3 to 3-8
  symbols in, 3-5
  syntax, 3-4
  troubleshooting, A-14
broadcast address, 1-8
bs (boot size) tag, in bootptab, 3-7

C

clocking, synchronous interface, 5-5
commands
  bconfig
    correcting router parameters with, A-2
    examples, 5-3
    for Local Boot, B-14
    format, 5-2
  boot, Local Boot, B-14
  get, A-8
  getcfg, 5-9, A-2, A-10
  ifconfig, 5-4 to 5-8
  log, A-8
  run inst_arn.bat
    See Quick-Start procedure
  run install.bat
    See Quick-Start procedure
compacting files, A-18
comparing startup options
  initial boot, 2-1
  routine boot, 2-3
compliance, Ethernet, C-3
CompuServe, Bay Networks forum on, xxx
config file. *See* configuration file
configuration file

- corrupted, A-17
- creating, 4-2
- customized, 1-5, 1-13, 2-3
- getting from a BOOTP server, 1-10 to 1-12
- hint for creating, C-1
- preparing, 4-2
- restrictions, 4-2
- T130 size tag, 3-6
- using local, B-14

configuring
- Directed Netboot, 3-1, 5-1
- EZ-Install, 3-1, 4-1
- interface, 5-2
- Local Boot, B-1
- Netboot, 3-1, 5-1
- network, C-3 to C-9

connecting multiple ANHs, C-6 to C-9

Connector IP Address parameter, 4-14

Connector Next Hop parameter, 4-14

Connector parameter, 4-12

Connector Protocol Mask parameter, 4-15

Connector State parameter, 4-15

Connector Subnet Mask parameter, 4-14

cost of line usage, 1-4, 2-4

Customer Service FTP, xxix

customer support. *See* getting help

D

daemon
- BOOTP, 3-2
- TFTP, 3-9

DCM
- configuring, 7-13, 7-15
- disabling, 7-12
- installing, 7-6
- parameters, 7-7
- reboot, 7-13
- rebooting, 7-7

DCMMW (DCM middleware), 7-2

debugging the BOOTP server, A-12

default IP interface settings
- Ethernet, 5-6, 5-7
- synchronous, 5-5

deleting files, A-16

dialup access, A-8

direct access. *See* Frame Relay

Directed Netboot
- bconfig command, 5-3
- configuring
  - boot client, 5-1
  - interfaces for, 4-1
  - server location, 5-2
  - UNIX server, 3-1
- ifconfig command, 5-8
- requirements for, 1-5

DLCI and IP address pair
- creating in client interface table, 4-21 to 4-23
- example, 1-8

DLCI Number parameter, 4-23

DLCMI settings, 5-5

driver, displaying MIB entry for, A-7

E

erasing files, A-16

error messages, displaying, A-8

Ethernet
- compliance, C-3
- interfaces
  - configuring, 5-6
  - displaying MIB entry, A-7
  - ifconfig settings, 5-6
- segment lengths, C-4

Ethernet DCM option. *See* DCM

Ethernet History group, 7-4, 7-19

Ethernet Statistics group, 7-3, 7-19

Event group, 7-5, 7-23

Events Manager tool, A-8

executable (.exe) files. *See* application files

EZ-Install, 1-7 to 1-12

configuring, 3-1, 4-1
initial startup option, 2-6
maximum PVCs, C-2
requirements, 1-4
summary, 1-3, 1-4
troubleshooting, A-2 to A-5

F

failure, BOOTP, A-2, A-3
FDDI interface limitation, C-2
fiber optic backbone, C-8
files
corrupted, A-17
naming restrictions, 4-3
transferring. *See* TFTP
Filter group, 7-4, 7-22
Flash memory, Local Boot image source, 1-5
format command, A-16
forwarding table. *See* BOOTP
Frame Relay
direct access PVC, 1-7
group access PVC
example, 1-8
setting up, 4-21 to 4-23
settings, 5-5
worksheet, B-11
frames, displaying, A-15

G

gateway, 4-16
get command, A-8
getcfg command, 5-6, 5-7, 5-9, A-2, A-10
getting help
from a Bay Networks Technical Response Center, xxxi
from the Support Source CD, xxx
through CompuServe, xxx
through Customer Service FTP, xxix
through InfoFACTS service, xxxi
through World Wide Web, xxix
group access. *See* Frame Relay

H

hd (home directory) tag, in bootptab, 3-6
HDLC encapsulation, 5-5
History Control group, 7-4, 7-19
home directory tag, 3-6
Host group, 7-4, 7-20
HostTopN group, 7-4, 7-21
HP 9000. *See* HP-UX
HP-UX
adding a TFTP user, 3-11
BOOTPD, 3-2
TFTPD access, 3-10

I

ifconfig command, 5-4
Image Builder default directory, 4-6
image, software
corrupted, A-17
generating, 4-6
getting from a BOOTP server, 1-10 to 1-12
preparing, 4-6
specifying location of, 5-2
transferring, C-2
upgrading, A-17
implementation notes, 7-16, C-2
incoming interface, specifying, 4-17 to 4-20
inetd.conf file
editing, 3-3
loading changes, 3-12
setting up static routes, 3-12
troubleshooting, A-4
InfoFACTS service, xxxi
initial startup options, 2-1
Input IP Address parameter, 4-20
interfaces

BOOTP parameters, 4-20
incoming and outgoing, 4-17 to 4-20
interoperability issues for RMON, 7-16
IP address
assigning manually, 2-7
DLCI, 4-21 to 4-23
failure, A-2
getting automatically, 1-7 to 1-9
input parameter, 4-20
manual assignment, 5-4
options for getting
EZ-Install, 1-7, 5-4
Local Boot, 1-5, 1-13, 2-3
Netboot or Directed Netboot, 5-4
output parameter, 4-20
tag, 3-5
IP interface
Ethernet
address settings, 5-6, 5-7
connector setting, 5-6, 5-7
synchronous
connector setting, 5-5
default settings, 5-5
IP routes
changing, 3-11
displaying, A-15
ip tag, in bootptab, 3-5

K

kernel file, 1-2
krnl_an.exe file
generating, 4-6
in router software image, 1-2
specifying instead of an.exe, A-3
upgrading, A-17
verifying as boot image, A-3
krnl_arn.exe file
generating, 4-6
in router software image, 1-2
specifying instead of arn.exe, A-3
upgrading, A-17
verifying as boot image, A-3

L

LAN protocol analyzer, A-9
line usage, minimizing
bandwidth, 2-5
cost, 2-4
link module, B-3
linking ANHs, C-6 to C-9
linking BOOTPD and TFTPD, 3-10
LMI, Frame Relay, 5-5
Local Boot
configuring, B-1
definition, 1-3
initial startup option, 2-9
starting, B-14
summary, 1-5
local file system, mounting, B-14
log command, A-8

M

Matrix group, 7-4, 7-21
memory
allocation hints, C-2
preventing saturation, 1-4, 2-4
use for RMON, 7-18
minimizing cost of line usage, 1-4, 2-4

N

naming configuration files, 4-3
Netboot
adding an interface for, 4-11 to 4-15
bconfig command, 5-2
configuring, 3-1, 4-1, 5-1, 5-2
definition, 1-3
requirements for, 1-4
summary, 1-4
troubleshooting, A-3 to A-5

Netboot Global parameters
Boot Config From Network, 4-9
Boot Config Pathname, 4-10
Boot Image From Network, 4-8
Boot Image Pathname, 4-10
Boot Server Address, 4-9
editing, 4-7 to 4-10
Netboot Interface parameters
Connector, 4-12
Connector IP Address, 4-14
Connector Next Hop, 4-14
Connector Protocol Mask, 4-15
Connector State, 4-15
Connector Subnet Mask, 4-14
Slot Number, 4-12
netstat command, 3-12, A-15
network analyzer, A-9
next-hop router
configuring, 4-21
not receiving BOOTP requests, A-2, A-3
not sending BOOTP responses, A-2, A-4

O

operating systems, 3-2
options for getting startup files
application files, 1-2
Directed Netboot, 1-5
EZ-Install, 1-4
Local Boot, 1-5
Netboot, 1-4
string files, 1-2
options for getting the IP address
Directed Netboot, 1-6
EZ-Install, 1-7
Local Boot, 1-13, 2-3
Netboot, 1-6
Optivity, 1-1
OSPF, worksheet for, B-7
outgoing interface, specifying, 4-17 to 4-20

P

Packet Capture group, 7-5, 7-22
Packet Capture tool, A-9
packets
analyzing, A-9
displaying forwarded and dropped, A-15
PathMan, 1-1
pathname restrictions, 4-3
pointer tag, in bootptab, 3-6
pound sign in bootptab file, 3-4
power loss while writing to a file, 2-4, A-17
PPP (Bay Networks Proprietary) wide-area protocol, worksheet for, B-10
PPP wide area protocol, worksheet for, B-12
PVC. *See* Frame Relay

Q

Quick Get tool, A-8
Quick-Start procedure
commands, B-14
defined, B-1
inst_arn.bat, B-14
install.bat script, B-14
using, B-14
worksheet, B-3 to B-6

R

rebooting the DCM, 7-7
receive socket, BOOTP, 3-2
relay agent forwarding table. *See* BOOTP
remote dialup, A-8
repeater ports, Ethernet
enabling, 6-1
resetting, 6-5
testing, 6-5
Request for Comments 1757, 7-1, 7-3
Reset parameter, 6-5

resetting and testing ANH, 6-1 to 6-5
resetting while writing to a file, 2-4, A-17
RFC 1048, 3-7
RIP routing protocol, worksheet for, B-6
RMON
  agent, 7-3
  control parameters, 7-3
  control tables, 7-3
  data tables, 7-3
  groups, 7-3 to 7-5
  interoperability issues, 7-17 to 7-23
  memory use, 7-18
RMON Default Host parameter, 7-10
RMON Default Matrix parameter, 7-11
RMON Max Host parameter, 7-10
router software image, definition of, 1-2
RouterMan, 1-1
routine startup options, 2-3
RS/6000. *See* AIX operating system

S

saturation of router memory, preventing, 2-4
Selftest, ANH parameter, 6-5
send socket, BOOTP, 3-2
slot number, B-3
Slot Number parameter, 4-12
sm (subnet mask) tab, in bootptab, 3-5
SMDS wide-area protocol, worksheet for, B-13
sniffer. *See* LAN protocol analyzer
SNMP implementation notes, 7-16
sockets, BOOTP, 3-2
software, configuration
  Diagnostics Monitor, 1-2
  Site Manager, 1-1
  Technician Interface, 1-1
Solaris
  copying BOOTPD, 3-2
  TFTPD access, 3-10
SQE test, disabling for AUI port, C-8
startup options
  displaying, 5-9, A-10
  initial, 2-1
    EZ-Install, 2-6
    Local Boot, 2-9
    Netboot, 2-7, 2-8
  Local Boot, 1-12
  Netboot, 1-6
  routine
    Directed Netboot, 2-4
    Local Boot, 2-5
    Netboot, 2-3
  selecting, 2-1
    Local Boot, 2-3, 2-5, 2-6
    Netboot, 2-3, 2-6
static routes to next-hop routers, setting up, 3-11
Statistics Manager tool, A-8
string files
  definition, 1-2
  generating, 4-6
subnet mask tag, 3-5
Sun workstations, 3-2
SunOS
  copying BOOTPD, 3-2
  TFTPD access, 3-10
Support Source CD, xxx
symbols in bootptab file, 3-4
synchronous interfaces
  configuring, 5-4
  displaying MIB entry, A-7
  ifconfig settings, 5-4
syntax of bootptab file, 3-4
System Administration Manager, HP 9000, 3-11

T

T130 size tag, in bootptab, 3-6
table continuation tag, 3-6
tags in bootptab
  definition, 3-6

format, 3-4
tc (table continuation) tag, in bootptab, 3-6
technical support, xxxi
TELNET, B-5
testing
BOOTP, C-1
IP interface during Quick-Start, B-16
TFTP
adding an HP 9000 user, 3-11
default volume, B-5
example, 1-11, 1-12
interruption, A-17
transferring image, C-2
TFTPD
linking to BOOTPD, 3-10
setting up, 3-9 to 3-13
tg variable in bootptab file, 3-4
Timeout Secs. parameter, 4-18
Token Ring interfaces
configuring, 5-6
ifconfig settings, 5-6
limitation, C-2
troubleshooting, A-1 to A-16

U

UDP, 3-2
underscore symbol in bootptab file, 3-5
UNIX workstation, 3-1
upgrading image, A-17
upstream router
definition, 4-21
not receiving BOOTP requests, A-2, A-3
not sending BOOTP responses, A-2, A-4
receiving IP address from, 1-7

V

vendor magic field, 3-7, A-13
versions of software, 2-6, 2-7, 4-6, C-2
vm (vendor magic) tag, in bootptab, 3-7
volume, specifying, A-17

W

wfBootpRelayIntfEntry, A-16
wfCSMACDEntry, A-7
wfDrivers, A-7
wfSyncEntry, A-7
wfTokenRingEntry, A-7
World Wide Web, Bay Networks home page on, xxix